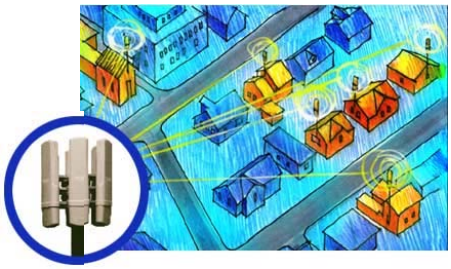
MOTOROLA
intelligence everywhere™



Canopy™ Bandwidth and Authentication Manager (BAM)

User Guide

BAM020-UG-en
Issue 5
June 2004

CANOPY™
Motorola Wireless Broadband Platform

BETA DRAFT

NOTICES

Software License Terms and Conditions

ONLY OPEN THE PACKAGE, DOWNLOAD OR USE THE SOFTWARE AND RELATED PRODUCT IF YOU ACCEPT THE TERMS OF THIS LICENSE. BY BREAKING THE SEAL ON THIS DISK KIT / CDROM, DOWNLOADING THE SOFTWARE FROM THE INTERNET, OR USING THE SOFTWARE OR RELATED PRODUCT, YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SOFTWARE OR RELATED PRODUCT; INSTEAD, DESTROY OR RETURN THE SOFTWARE IF PURCHASED FOR A FULL REFUND. THE FOLLOWING AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR ENTITY), AND MOTOROLA, INC. (FOR ITSELF AND ITS LICENSORS). THE RIGHT TO USE THIS PRODUCT IS LICENSED ONLY ON THE CONDITION THAT YOU AGREE TO THE FOLLOWING TERMS.

Now, therefore, in consideration of the promises and mutual obligations contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby mutually acknowledged, you and Motorola agree as follows:

Grant of License. Subject to the following terms and conditions, Motorola, Inc., grants to you a personal, revocable, non-assignable, non-transferable, non-exclusive and limited license to use on a single piece of equipment only one copy of the software rightfully obtained by you from Motorola (Software). You may make two copies of the Software, but only for backup, archival, or disaster recovery purposes. On any copy you make of the Software, you must reproduce and include the copyright and other proprietary rights notice contained on the copy we have furnished you of the Software.

Ownership. Motorola (or its supplier) retains all title, ownership and intellectual property rights to the Software and any copies, including translations, compilations, derivative works (including images) partial copies and portions of updated works. The Software is Motorola's (or its supplier's) confidential proprietary information. This Software License Agreement does not convey to you any interest in or to the Software, but only a limited right of use. You agree not to disclose it or make it available to anyone without Motorola's written authorization. You will exercise no less than reasonable care to protect the Software from unauthorized disclosure. You agree not to disassemble, decompile or reverse engineer, or create derivative works of the Software, except and only to the extent that such activity is expressly permitted by applicable law.

Termination. This License is effective until terminated. This License will terminate immediately without notice from Motorola or judicial resolution if you fail to comply with any provision of this License. Upon such termination you must destroy the Software, all accompanying written materials and all copies thereof, and the sections entitled Limited Warranty, Limitation of Remedies and Damages, and General will survive any termination.

Limited Warranty. Motorola warrants for a period of ninety (90) days from Motorola's or its customer's shipment of the Software to you that (i) the disk(s) on which the Software is recorded will be free from defects in materials and workmanship under normal use and (ii) the Software, under normal use, will perform substantially in accordance with Motorola's published specifications for that release level of the Software. The written materials are provided "AS IS" and without warranty of any kind. Motorola's entire liability and your sole and exclusive remedy for any breach of the foregoing limited warranty will be, at Motorola's option, replacement of the disk(s), provision of downloadable patch or replacement code, or refund of the unused portion of your bargained for contractual benefit up to the amount paid for this Software License.

THIS LIMITED WARRANTY IS THE ONLY WARRANTY PROVIDED BY MOTOROLA, AND MOTOROLA AND ITS LICENSORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OF IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. MOTOROLA DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN REPRESENTATIONS MADE BY MOTOROLA OR AN AGENT THEREOF SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. MOTOROLA DOES NOT WARRANT ANY SOFTWARE THAT HAS BEEN OPERATED IN EXCESS OF SPECIFICATIONS, DAMAGED, MISUSED, NEGLECTED, OR IMPROPERLY INSTALLED. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Limitation of Remedies and Damages. Regardless of whether any remedy set forth herein fails of its essential purpose, IN NO EVENT SHALL MOTOROLA OR ANY OF THE LICENSORS, DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES OF THE FOREGOING BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL,

INDIRECT, SPECIAL OR SIMILAR DAMAGES WHATSOEVER (including, without limitation, damages for loss of business profits, business interruption, loss of business information and the like), whether foreseeable or unforeseeable, arising out of the use or inability to use the Software or accompanying written materials, regardless of the basis of the claim and even if Motorola or a Motorola representative has been advised of the possibility of such damage. Motorola's liability to you for direct damages for any cause whatsoever, regardless of the basis of the form of the action, will be limited to the price paid for the Software that caused the damages. THIS LIMITATION WILL NOT APPLY IN CASE OF PERSONAL INJURY ONLY WHERE AND TO THE EXTENT THAT APPLICABLE LAW REQUIRES SUCH LIABILITY. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Maintenance and Support. Motorola shall not be responsible for maintenance or support of the software. By accepting the license granted under this agreement, you agree that Motorola will be under no obligation to provide any support, maintenance or service in connection with the Software or any application developed by you. Any maintenance and support of the Related Product will be provided under the terms of the agreement for the Related Product.

Transfer. In the case of software designed to operate on Motorola equipment, you may not transfer the Software to another party except: (1) if you are an end-user, when you are transferring the Software together with the Motorola equipment on which it operates; or 2) if you are a Motorola licensed distributor, when you are transferring the Software either together with such Motorola equipment or are transferring the Software as a licensed duly paid for upgrade, update, patch, new release, enhancement or replacement of a prior version of the Software. If you are a Motorola licensed distributor, when you are transferring the Software as permitted herein, you agree to transfer the Software with a license agreement having terms and conditions no less restrictive than those contained herein. You may transfer all other Software, not otherwise having an agreed restriction on transfer, to another party. However, all such transfers of Software are strictly subject to the conditions precedent that the other party agrees to accept the terms and conditions of this License, and you destroy any copy of the Software you do not transfer to that party. You may not sublicense or otherwise transfer, rent or lease the Software without our written consent. You may not transfer the Software in violation of any laws, regulations, export controls or economic sanctions imposed by the U.S. Government.

Right to Audit. Motorola shall have the right to audit annually, upon reasonable advance notice and during normal business hours, your records and accounts to determine compliance with the terms of this Agreement.

Export Controls. You specifically acknowledge that the software may be subject to United States and other country export control laws. You shall comply strictly with all requirements of all applicable export control laws and regulations with respect to all such software and materials.

U.S. Government Users. If you are a U.S. Government user, then the Software is provided with "RESTRICTED RIGHTS" as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at FAR 52 227-19 or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, as applicable.

Disputes. You and Motorola hereby agree that any dispute, controversy or claim, except for any dispute, controversy or claim involving intellectual property, prior to initiation of any formal legal process, will be submitted for non-binding mediation, prior to initiation of any formal legal process. Cost of mediation will be shared equally. Nothing in this Section will prevent either party from resorting to judicial proceedings, if (i) good faith efforts to resolve the dispute under these procedures have been unsuccessful, (ii) the dispute, claim or controversy involves intellectual property, or (iii) interim relief from a court is necessary to prevent serious and irreparable injury to that party or to others.

General. Illinois law governs this license. The terms of this license are supplemental to any written agreement executed by both parties regarding this subject and the Software Motorola is to license you under it, and supersedes all previous oral or written communications between us regarding the subject except for such executed agreement. It may not be modified or waived except in writing and signed by an officer or other authorized representative of each party. If any provision is held invalid, all other provisions shall remain valid, unless such invalidity would frustrate the purpose of our agreement. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent action in the event of future breaches.

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright and Licensing Information for ACE™, TAO™, and CIAO™

ACE™, TAO™, and CIAO™ are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University Copyright (c) 1993-2003, all rights reserved.

ACE+TAO+CIAO are provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, ACE+TAO+CIAO are provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement.

gSOAP

Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RSA Data Security, Inc. MD5 Message-Digest Algorithm

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. Allrights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Other Software Licenses

It is strongly recommended that the operator purchase a license for Red Hat® Linux® operating system from Red Hat, Inc. and use support from Red Hat, Inc. Licensing information for Linux® software is available at http://www.redhat.com.

NOTE: For BAM Release 2.0 and later releases, Canopy no longer licenses the use of MySQL® software on the BAM server, but strongly recommends that customers who use MySQL® software comply with all of the licensing requirements of that product.

Licensing information for PHP software is available at http://www.php.net/license.
Licensing information for Apache™ Server software is available at http://www.apache.org/licenses.

Trademarks, Product Names, and Service Names

MOTOROLA, the stylized M Logo and all other trademarks indicated as such herein are trademarks of Motorola, Inc. ® Reg. U.S. Pat & Tm. Office. Canopy is a trademark of Motorola, Inc. All other product or service names are the property of their respective owners.

Motorola, Inc
Broadband Wireless Technology Center
1299 East Algonquin Road
Schaumburg, IL 60196
USA

http://www.motorola.com/canopy

TABLE OF CONTENTS

1 INTRODUCTION 9
1.1 Feedback 9
1.2 Technical Support 9
2 ABOUT THIS USER GUIDE 10
2.1 Intended Use 10
2.2 New in This Issue 10
2.3 Related Documents 11
3 PRODUCT DESCRIPTION 12
3.1 Services and Features Provided 12
3.1.1 Quality of Service—Bandwidth Management 12
3.1.2 Authentication 12
3.1.3 Graphical User Interface (GUI) 12
3.1.4 Network Flexibility 13
3.2 Hardware and Software Requirements 14
3.2.1 Software Compatibility 15
3.2.2 Software Upgrades 15
3.2.3 License Management 16
3.3 Applications in the Network 19
3.3.1 Authentication Feature 19
3.3.2 Typical Network with BAM 20
3.3.3 Engineering Rules 20
3.4 BAM Ports Used 21
4 CONCEPTS AND BACKGROUND 22
4.1 QoS Information 22
4.1.1 QoS Parameters 22
4.1.2 Bandwidth from the SM Perspective 23
4.1.3 Interaction of Burst Allocation and Sustained Data Rate Settings 23
4.1.4 Examples of Tiered Service Levels for SMs 24
4.2 Authentication 25
4.2.1 Authentication Process 25
4.2.2 Keys and Random Number 27
4.2.3 Log of Authentication Events 27
4.3 SQL Database 27
4.3.1 ESN Data Table 28
4.3.2 Canopy Data Formatter (CDF) Script for ESN Data Table Creation 29
4.3.3 Relationship of ESN Data Table, XML Data File, and SM Database 29
5 INSTALLATION AND OPERATION PROCEDURES 31
5.1 Installations and Tests 31
5.1.1 Acquire the Initial Software 31
5.1.2 Plan the Installations 31
5.1.3 Copy Essential Files to Alternate Media 32
5.1.4 Disable Authentication in Affected APs 33
5.1.5 Install Red Hat Enterprise Linux Version 3 33
5.1.6 Set up ODBC 35
5.1.7 Set Up License Management 35

5.1.8 Set Up BAM 35
5.2 Management of QoS and Authentication 40
5.2.1 Use the GUI to Change Subscriber Data 40
5.2.2 Use the GUI to Suspend or Reinstate Service to a Subscriber 41
5.2.3 Use the GUI to Back Up an ESN Data Table 42
5.2.4 Customize the GUI 43
5.2.5 Use the Command-line Interface to Change SM QoS Data 43
5.3 Configuration in the AP and SM 44
6 HISTORY OF CHANGES IN THIS DOCUMENT 45
APPENDIX 1: POSTGRESQL DATABASE SUPPORT 46
Set up BAM GUI for PostgreSQL Database 46
Test the ODBC Driver for PostgreSQL 48
Use a PostgreSQL Database 48
PostgreSQL Directories 48
PostgreSQL Documentation 48
Enable PostgreSQL on Red Hat Enterprise Linux Version 3 48
Configure PostgreSQL to Require Passwords 49
Change Password for PostgreSQL 49
Configure PostgreSQL to Use TCP/IP Sockets 49
Create Canopy User and Database 50
Use PostgreSQL Interactive Terminal Commands 50
Display Data 54
Reload PostgreSQL Configuration Data 54
Hazardous Command 54
APPENDIX 2: MYSQL DATABASE SUPPORT 55
Set up BAM GUI for MySQL Database 55
Test the ODBC Driver for MySQL 57
Replicate MySQL Database on Redundant Server 57
Caveats about Database Replication 57
Set Up Automatic Replication 57
Verify BAM Redundancy 62
APPENDIX 3: SSE COMMAND-LINE INTERFACE 63
Caveats 63
SSE Database Commands 63
SSE telnet Commands 65
APPENDIX 4: RADIUS SERVER SUPPORT 67
RADIUS Fields in canopyapi.xml 67
Set up RADIUS on BAM Server 68
Set up BAM on RADIUS Server 69
APPENDIX 5: TROUBLESHOOTING 71
Other Messages 71

LIST OF FIGURES

Figure 1: Example GUI page, BAM Release 2.0 13
Figure 2: BAM Release 2.0 in a typical Canopy network 19
Figure 3: Greater Burst Allocation value 23
Figure 4: Equal Burst Allocation value 24
Figure 5: Authentication message flow 26
Figure 6: Typical ESN Data Table, Columns 1, 2, and 3 29
Figure 7: Typical ESN Data Table, Columns 1 and 2 29
Figure 8: Typical ESN Data Table, Column 3 29
Figure 9: Database inputs and outputs without cdf script 30
Figure 10: Database inputs and outputs with cdf script 30
Figure 11: Example session to preserve ESN Data Table 32
Figure 12: Activating or suspending access for the subscriber 41
Figure 13: Access suspended for the subscriber 42

LIST OF TABLES

Table 1: Quick reference 10
Table 2: Compatibility of software releases 15
Table 3: Software upgrade paths 15
Table 4: BAM server ports 21
Table 5: Examples of SM tiers 24
Table 6: Definition of ESN Data Table fields 28
Table 7: Definitions of cdf script variables 39
Table 8: Example expressions for this procedure 58
Table 9: RADIUS fields 67
Table 10: Example problems for troubleshooting 71

1 INTRODUCTION

Thank you for your purchase of Canopy™ Bandwidth and Authentication Manager (BAM) software.[1] When you integrate this software with standard computer hardware and open source software, you have power and flexibility to manage both bandwidth and security on your Canopy network.

1.1 FEEDBACK

We welcome your feedback on Canopy system documentation. This includes feedback on the structure, content, accuracy, or completeness of our documents, and any other comments you have. Please send your comments to technical-documentation@canopywireless.com.

1.2 TECHNICAL SUPPORT

To get information or assistance as soon as possible for problems that you encounter, use the following sequence of action:

1. Search this document, the user manuals that support the modules, and the software release notes of supported releases
   a. in the Table of Contents for the topic.
   b. in the Adobe Reader® search capability for keywords that apply.[2]
2. Visit the Canopy systems website at http://www.motorola.com/canopy.
3. Search Red Hat® Enterprise Linux® operating system documentation at either http://www.redhat.com/docs/manuals/enterprise/.[3]
4. Ask your Canopy products supplier to help.
5. Gather information such as
   - the IP addresses and MAC addresses of any affected Canopy modules.
   - the software releases that operate on these modules.
   - data from the Event Log page of the modules.
   - the configuration of software features on these modules.
5. Escalate the problem to Canopy systems Technical Support (or another Tier 3 technical support that has been designated for you) as follows. You may either
   - send e-mail to technical-support@canopywireless.com.
   - call 1 888 605 2552 (or +1 217 824 9742) during the following hours of operation:
     Monday through Sunday
     7:00 a.m. to 11:00 p.m. EST

For warranty assistance, contact your reseller or distributor for the process.

[1] Canopy is a trademark of Motorola, Inc.
[2] Reader is a registered trademark of Adobe Systems, Incorporated.
[3] Red Hat is a registered trademark of Red Hat, Inc. Linux is a registered trademark of Linus Torvalds.

2 ABOUT THIS USER GUIDE

This user guide supports planning, installation, and operation of a BAM. Each of these functions requires much of the same information.

2.1 INTENDED USE

This manual should be used with Canopy features through Software Release 4.1. The audience for this manual comprises system operators, network administrators, and equipment installers. To find information based on a general question, use Table 1 for quick reference.

Table 1: Quick reference

To answer…	see…	to find…
What is BAM?	PRODUCT DESCRIPTION on Page 12	features, uses, terminology
How does BAM work?	CONCEPTS AND BACKGROUND on Page 22	theory, internal operation
How do I work with a BAM?	INSTALLATION AND OPERATION PROCEDURES on Page 31	procedures for the user
What commands are executed on the BAM server?	APPENDIX 3: SSE COMMAND-LINE INTERFACE on Page 63	lists and descriptions of commands

To find information based on any expression used in this document, open the document in an Adobe Reader session and

- use the page numbers at the bottom of the screen and in the thumbnails. These match the page numbers in the Table of Contents.
- use the **Edit** → **Search** command (**Ctrl+F**) to find a word or phrase.

2.2 NEW IN THIS ISSUE

Issue 5 introduces the following changes:

- Procedures to install software that BAM Release 2.0 requires.
- Removal of the caveat (from Issue 4, Section 5.2.8) that stated “before the procedure in Use the GUI to Change Subscriber Data can be used to add SMs, the ESN Data Table file must contain information for at least one SM.”
  NOTE: This caveat continues to apply in Release 1.1, but does not apply in Release 2.0.
- The section Interaction of Burst Allocation and Sustained Data Rate Settings on Page 23 recomposed for clarity.

- A procedure to set up automatic replication of a MySQL database in redundant BAM servers. See Replicate MySQL Database on Redundant Server on Page 57.
  NOTE: No automatic replication setup procedure is provided for a PostgreSQL database.
- Addition of APPENDIX 5: TROUBLESHOOTING on Page 71.
- Documentation of Release 2.0 features as follows:
  - Support for a PostgreSQL database (support is no longer limited to a MySQL database). See APPENDIX 1: PostgreSQL DATABASE SUPPORT on Page 46.
  - Capability to suspend services to an SM without deleting the configuration from the database. See Use the GUI to Suspend or Reinstate Service to a Subscriber on Page 41.
  - Option for the service provider to have a RADIUS server control authentication and bandwidth management with the BAM server as a proxy server.
    NOTE: In this case, the BAM GUI *cannot* manage the contents of the database. See APPENDIX 4: RADIUS SERVER SUPPORT on Page 67.
  - Server-based license management. See License Management on Page 16.
  - Removal of the Engine interface to SMs and APs. See APPENDIX 3: SSE COMMAND-LINE INTERFACE on Page 63.
  - Support for only Red Hat Enterprise Linux Version 3 operating system. See Hardware and Software Requirements on Page 14.

2.3 RELATED DOCUMENTS

The Canopy Subscriber Module (SM) and Access Point module (AP) are described in their User Manuals. Please refer to http://www.motorola.com/canopy for an overview of the Canopy system and for the latest versions of user manuals, user guides, and supporting information.

Integration and operation of BAM requires

- knowledge of IP networking. BAM can be integrated in any of several configurations, based on operator requirements, network design, and other factors. This user guide *does not* provide the requisite background in IP networking.
- guidance and tips on network integration and BAM installation. These are provided in this user guide.
- familiarity with standard computer hardware. See the user documentation that the manufacturer provides.
- familiarity with open source software. See the user documentation that the software supplier provides.

3 PRODUCT DESCRIPTION

This section describes

- the services and features that BAM provides.
- the hardware and software elements that BAM requires.
- the application of BAM in a Canopy network.

3.1 SERVICES AND FEATURES PROVIDED

The Canopy Bandwidth and Authentication Manager (BAM) provides the following services and features.

3.1.1 Quality of Service—Bandwidth Management

Per-Subscriber Module (SM) bandwidth can be set for a sustained rate and for a burst rate. With this capability, the Canopy system allows both

- burst rates beyond those of many other broadband access solutions.
- control of average bandwidth allocation to prevent excessive bandwidth usage by a subscriber.

All packet throttling occurs in the SMs (Subscriber Modules) and APs (Access Point Modules) based on Quality of Service (QoS) data that the BAM server provides. No BAM processing power or network messages are needed for packet throttling.

QoS management also supports marketing of broadband connections at various data rates, for operator-defined groups of subscribers, and at various price points. This allows the operator to meet customer needs at a price that the customer deems reasonable and affordable.

NOTE: In a network where VLAN tagging is applied, QoS information is displaced in the frame structure. For this reason, the high-priority channel is not available where VLAN tagging is applied.

3.1.2 Authentication

To control access to a Canopy system, each AP can be configured to require secure SM authentication before network access is allowed. This configuration allows individual management of authentication and keys for each SM.

3.1.3 Graphical User Interface (GUI)

When BAM Release 1.1 or later release operates on the BAM server, the server provides a GUI as well as a command line interface. This GUI uses a web browser to display pages of information in which the operator can easily change BAM data. These pages also display a table of the electronic serial numbers (ESNs) of all SMs in the BAM database. An example for BAM Release 2.0 is displayed in Figure 1.

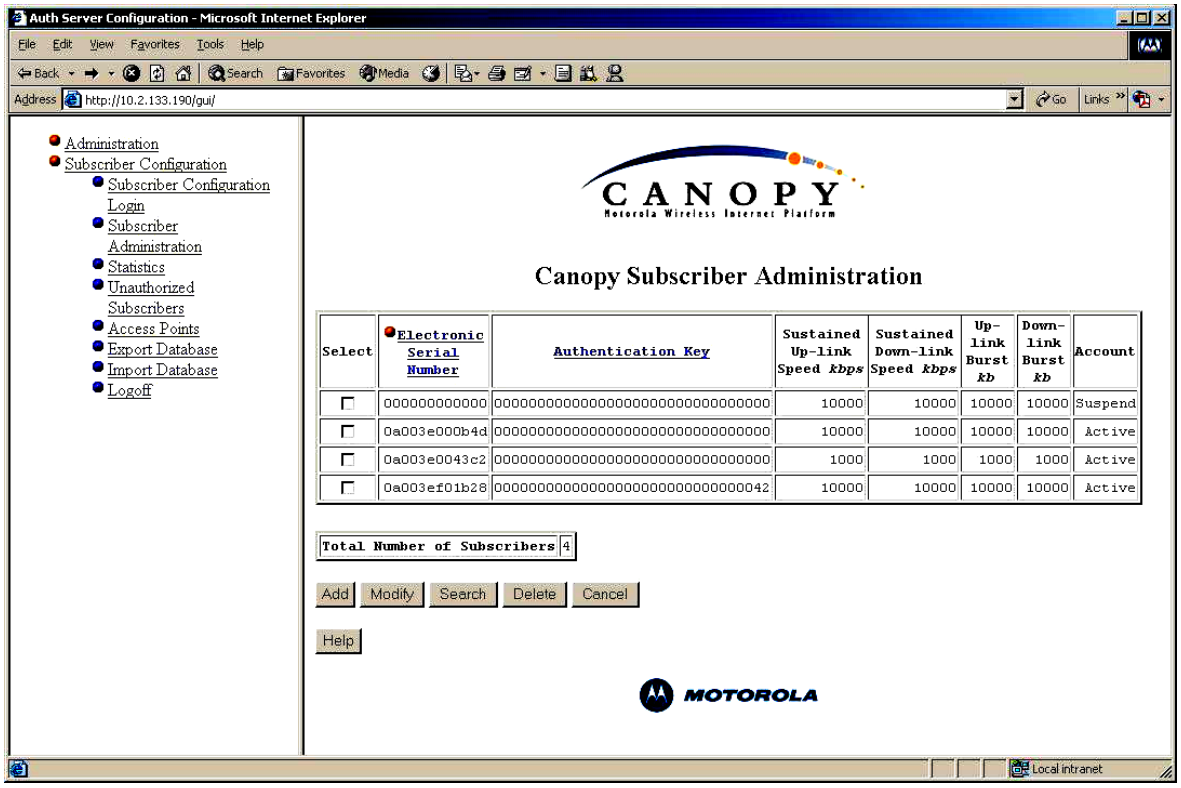


Figure 1: Example GUI page, BAM Release 2.0

Because the GUI is a web browser, you can access the GUI from any element in the network. However, this depends on the IP address of the BAM server (as routable) and on the network configuration.

IMPORTANT: In any BAM GUI session, to return to a previously loaded BAM web page, use the **back** button in the GUI rather than the Back button of your browser. Using the browser Back button causes the session to lose some settings and generate errors.

3.1.4 Network Flexibility

BAM architecture supports network flexibility. In the typical configuration, the operator deploys two BAM servers. The second provides backup in case the first fails. However, BAM can be operated on a single server or across multiple servers.

3.2 HARDWARE AND SOFTWARE REQUIREMENTS

The BAM server uses the following hardware and software elements:

- Bandwidth and Authentication Manager (BAM) software, commercial software licensed to the user from the Canopy division. This software comprises
  - SSE, the BAM command-line interface with the SQL database.
  - GUI, a graphical user interface for BAM.
- License management technology from Macrovision, based on the FLEXnet™ Publisher license management model[4] (in BAM Release 2.0 and later releases), platform licensed to the user from the Canopy division.[5] Thus, BAM is a *FLEXenabled* product.
- CPU(s)—provided by the operator. A recommended computer is the Dell™ OptiPlex™ GX150 with an Intel® Pentium® III processor, 256 MB of memory, and 20-GB hard drive, or an equivalent.[6]
- Red Hat Enterprise Linux Version 3 operating system—open source software distributed by Red Hat, Inc. and obtained by the operator (see http://www.redhat.com).

  BAM Release 2.0 uses the following software and files, some of which are included in the Red Hat Enterprise Linux Version 3 operating system distribution:
  - Open Database Connectivity (ODBC) interface—*required* by BAM Release 2.0 and later releases to interoperate with the database.[7]
  - PHP software—*required* open source software that BAM uses to create and manage web pages as part of the GUI.[8]
  - Apache™ Server (with `httpd` service script) software—*required* by BAM to present the web pages that are built by PHP software and the database.[9]
  - optionally, MySQL® software—open source software from the MySQL AB Company to support a MySQL database with BAM Releases 2.0.[10]
    NOTE: Before the introduction of BAM Release 2.0, MySQL licensing and integration rules changed. In BAM release 2.0 and later releases, if you wish to maintain a MySQL database, you must access the database through the ODBC interface. The MySQL driver that you may have used with BAM Release 1.1 *is not* supported. This change allows you to use whatever version of MySQL software you are entitled to and wish to use.
  - optionally, PostgreSQL® software—open source software from PostgreSQL, Inc. to support a PostgreSQL database (accessed through ODBC) with BAM Release 2.0 and later releases.[11]

[4] FLEXnet is a trademark of Macrovision Corporation.
[5] This license server software may be local or remote. However, an odd number of servers running this software is required for license assignments and license checking and a majority of these must agree on any assignment determination.
[6] Dell and OptiPlex are trademarks of Dell, Inc.
Intel and Pentium are registered trademarks of Intel Corporation.
[7] See http://www.unixodbc.org/.
[8] PHP is a scripting language project of the Apache Software Foundation.
[9] Apache is a trademark of the Apache Software Foundation, and is used with permission.
[10] MySQL is a registered trademark of the MySQL AB Company in the United States, the European Union, and other countries.
[11] PostgreSQL is a registered trademark of PostgreSQL, Inc.

For more information about distributions of BAM Release 2.0 and associated software/licenses, see Software and License Distribution on Page 9.

3.2.1 Software Compatibility

The compatibility of BAM software, Red Hat Linux operating system, and Canopy system software releases is indicated in Table 2.

Table 2: Compatibility of software releases

BAM	Red Hat Linux OS	Canopy System
1.0	7.3	3.1.x
1.1	9 or Enterprise Version 3 (WS or ES)	3.1.x through 4.2
2.0	Enterprise Version 3 (WS or ES)	4.x through 6.x

3.2.2 Software Upgrades

Software upgrades can be performed as indicated in Table 3.

Table 3: Software upgrade paths

Software	From Release	To Release	Upgrade Path Exists	Where Documented
BAM application	1.0	1.1	yes	BAM User Guide Issue 4, January 2004
	1.1	2.0	yes[1]	Installations and Tests on Page 31
Red Hat Linux OS	7.3	9	yes	http://www.redhat.com/docs/manuals/linux/
	9	Enterprise Version 3 (WS or ES)	no	http://www.redhat.com/docs/manuals/enterprise/ See also Install Red Hat Enterprise Linux Version 3 on Page 33

NOTES:

1. Only where Red Hat Enterprise Linux Version 3 had been the operating system on the BAM server when BAM Release 1.1 was installed.

3.2.3 License Management

License Management Sequence

In BAM Release 2.0 and later releases, the process of license management is as follows:

1. The operator
    a. designates one or any greater *odd* number of servers to, in addition to possible other functions, act as license servers.
    NOTE: Any of these servers can operate on the Red Hat Linux 9, Enterprise Linux, or MS-Windows operating system. In addition, any of these servers can also be BAM servers.
    b. identifies the maximum number of APs that will need to simultaneously use a floating license.
    c. identifies the maximum number of servers that will need to simultaneously use a BAM server floating license. (For BAM server license considerations, see BAM Server and AP Authentication License Planning on Page 18.)
    d. submits an order that indicates both the number and type of floating licenses and the hostID (MAC address) of each server that will be used as a license server (typically, a single server; three for redundancy on license servers).
    NOTE: Previous APAS keys are fully credited toward acquisition of floating AP authentication licenses.
    e. receives the license keys for the BAM server and AP authentication.
    f. installs the license manager software onto each designated license server (identified in Step 1a).
    g. installs the license keys for BAM server and AP authentication into each designated license server.
    NOTE: Although the run-time use of these licenses is floating in the network, these licenses are node locked to the hostID (MAC address) of the license server.

    NOTE: Messages that are exchanged in the following sequence are recorded on the BAM server in the `/var/log/canopy/canopy.log` file. However, the BAM server does not display these messages.
2. When BAM software boots, the active BAM server calls the license server(s) for a floating BAM server license.
3. If the majority of license servers find that no BAM server floating license remains unassigned, then they reject the license request.

    If the majority of license servers find that a floating BAM server floating license is unassigned, then they assign a license to the BAM server.

    NOTE: Where three license servers are deployed, if one goes out of service, the two that remain in service continue license management (because a majority of the deployment is still able to govern). When BAM cannot call the license server, requests for new licenses are rejected, but previously assigned licenses remain effective.
4. BAM tracks the licenses that are assigned to APs that have called the BAM server.

5. At regular intervals, the BAM server `pings` each AP on its license tracking list. If an AP fails to respond to a `ping`, then the BAM server returns the license previously held by that AP to the license server.
6. Messaging and licensing proceed as described under Authentication Process on Page 25.

License Forfeiture and Reassignment

As described in the sequence above, an AP that holds a floating license and fails to respond to a `ping` request from the BAM server forfeits its floating license. What is significant in this case is that the AP has failed to respond to the `ping`.

- If the failure to respond is a symptom of the AP being out of service, then no subscriber for that AP is being served.
- If the AP is not out of service and is still set to require authentication, then no subscriber who attempts to register (or attempted to register since communication with the BAM server was lost) can be served.

These significant problems are not caused by license administration. If the number of AP floating licenses is equal to the number of APs that simultaneously are set to require authentication, then a floating license is available in the license server for the AP that forfeited one by failing to respond to the `ping`.

If an AP that is set to require authentication and associates with a BAM server goes out of service and you cannot put the AP back into service, you can

- replace the AP with
  - any available AP that is of device type Access Point Authentication Server (APAS) and operating on a Canopy system release earlier than Release 4.2.3.
  - any available AP that is operating on Release 4.2.3 or a later release.
- set the replacement AP to require authentication.
- identify the IP address of the BAM server(s) that the AP should call.

The first subsequent time that an SM attempts to register in the replacement AP, license management proceeds as follows:

1. The AP calls the primary BAM server.
2. BAM checks the list of assigned licenses and ascertains that the license that was previously assigned to the AP that went out of service is not currently assigned.
3. The BAM server calls the license management server.
4. The license management server assigns the previously assigned license.
5. The BAM server associates this license with the replacement AP and permits the current and subsequent authentication attempts.

BAM forfeits its BAM server floating license only when the server goes out of service. In this case, the license management server places into the available license pool

- the license of the BAM server that went out of service.
- the licenses of all APs that were licensed through that BAM server.

BAM Server and AP Authentication License Planning

Planning the number of required AP authentication floating licenses is simple, as implied above. Only the number of APs (not the identity of them) that may simultaneously require the functionality must be identified.

Planning the number of required BAM server licenses is subject to the implementation and backup capability that you have engineered. For example, in a Canopy network where you implement three associated BAM servers, you can acquire

- one floating BAM server license that will be available to the backup BAM server only if the primary BAM server goes out of service. This carries the risk that, if the primary BAM server simply loses network connectivity and then authentication requests are automatically transferred to the secondary BAM server, the secondary BAM server cannot assume the license of the primary BAM server.
- two floating BAM server licenses—one for the primary and one for the secondary BAM server. This *does not* carry the risk that is inherent in having only one BAM server floating license. Until the primary is put back into service, the secondary becomes the primary, and the tertiary becomes the secondary. The backup protection perpetuates.
- three floating BAM server licenses. This provides simultaneous functionality to all three, which can then participate in load balancing.

Software and License Distribution

Each BAM Release 1.0 or 1.1 customer automatically receives a distribution of

- as many BAM server floating licenses as the previously purchased BAM server license keys.
- as many AP authentication floating licenses as the previously purchased APAS license keys.

Each customer who *has not* previously purchased BAM software and APAS keys or who is extending BAM capability to additional servers and APs receives, upon order

- BAM server floating licenses as ordered.
- AP authentication floating licenses as ordered.
- as many APAS license keys (for the APs) as the AP floating licenses ordered before Release 4.2.3 is available.

In addition, the customer must provide the hostID (MAC address) of the license server(s) with each order for BAM server floating licenses and AP authentication floating licenses.

BAM Release 2.0 and license management server software are available for download from the Canopy web site at the convenience of the user.

IMPORTANT: In Canopy system releases earlier than Release 4.2.3, each AP that communicates with the BAM server must have an APAS license key installed on the radio in addition to an active floating license that the license management server has assigned. In these earlier system releases

- an available BAM server floating license authorizes any server
- an available AP floating license authorizes only an APAS.

3.3 APPLICATIONS IN THE NETWORK

An example application of BAM in a Canopy network is illustrated in Figure 2.

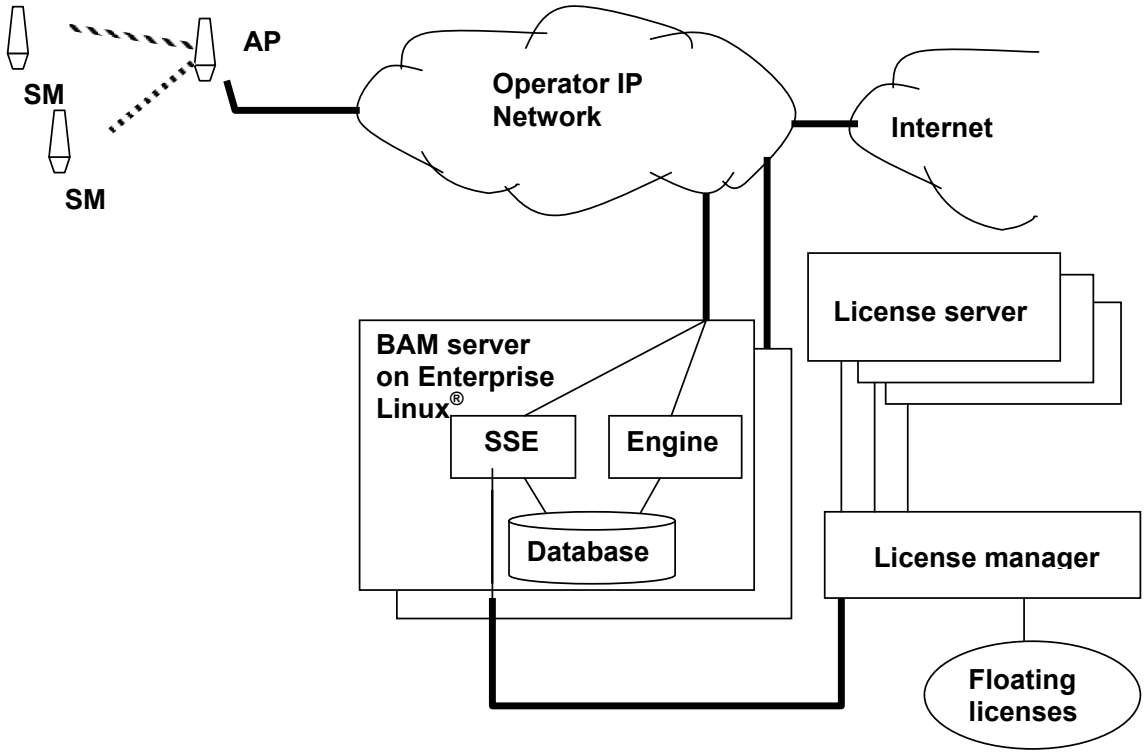


Figure 2: BAM Release 2.0 in a typical Canopy network

3.3.1 Authentication Feature

The operator enables the Authentication feature per AP. When this feature is enabled in an AP, any SM that attempts registration to the AP is denied service if authentication fails, such as (but not limited to) when no BAM server is operating or when the SM is not listed in the database. If a BAM server drops out of service, an SM that is already in session remains in session, but an SM that attempts to register is denied service. In a typical Canopy network, some SMs re-register daily (when subscribers power down the SMs, for example), and others do not re-register in a period of several weeks.

When authentication fails, the SM locks out of any other attempt to register to same AP in the next 15 minutes.

3.3.2 Typical Network with BAM

The following configuration is typical in a Canopy network with BAM:

- Two Linux operating system servers are deployed. Each operates all of the software, with IP addresses set so that APs can access each server. In this case, if one BAM server fails, SMs can register to the other BAM server and are not denied service.
  - The BAM servers are topologically separated on the operator network. The BAM servers may be geographically near each other but, from the network perspective, should be separate. This reduces the risk that the failure of a network element denies connectivity to *both* BAM servers.
  - The BAM servers are topologically near the operator gateway to the Internet. This also reduces the risk that the failure of a network element denies connectivity to the BAM servers.
- An odd number of license management servers.

3.3.3 Engineering Rules

The network planner may engineer an alternative BAM configuration that complies with the following rules:

- Each BAM server must operate on the Red Hat Enterprise Linux Version 3 operating system.
- BAM SSE software may operate on its own server.
- The MySQL or PostgreSQL database may reside on its own server.
- Each AP can communicate with as many as three BAM Engines.
- The license management software may operate on the same server as the BAM or on a different server.

In each case, the assignment of multiple IP addresses on the AP Configuration web page allows the use of multiple BAM servers, and the protocol ensures attempts to reach an alternative server when no response is received from the first.

3.4 BAM PORTS USED

The ports that are used for BAM are listed in Table 4. These ports are also listed in the `/etc/services` file.

Table 4: BAM server ports

Alias[1]	Port	Description
engined	9090/tcp[2]	Engine Port (Not used in BAM Release 2.0 and later releases.)
ap	1234/udp[3]	AP Port (For communication between BAM and APs. Must remain open where firewall is used.)
canopyapi	60616/tcp[2]	SOAP API Port (For communication between SSE and Engine.)
apserver	61001/udp[3]	AP List Port (Port on AP, not on BAM server.)
ssed	9080/tcp[2]	SSE Port

1. BAM addresses each port by alias within (and only within) the BAM server. The alias is helpful in a case where other software uses the same port.
2. Keep inside of the firewall.
3. Keep outside of the firewall.

4 CONCEPTS AND BACKGROUND

This section describes

- the settable parameters that control SM bandwidth.
- the depletion and recharge of bandwidth capability for the SM.
- examples of configurable service levels for tiers of subscriber bandwidth needs.

4.1 QOS INFORMATION

When an SM registers to an AP during the authentication process, QoS information can be provided to the SM and the AP. The SM and the AP then use this information for bandwidth management. This process is described under Authentication Process on Page 25.

4.1.1 QoS Parameters

The four parameters included in bandwidth management are

- **Sustained Uplink Data Rate** (kbps).
- **Uplink Burst Allocation** (kb).
- **Sustained Downlink Data Rate** (kbps).
- **Downlink Burst Allocation** (kb).

You can independently set each of these parameters per AP (with or without BAM) or per SM (with BAM).

Token Buckets

The Canopy software uses theoretical *token buckets* to manage the bandwidth of each SM. Each SM employs two buckets: one for uplink and one for downlink throughput. These buckets are continuously being filled with tokens at rates set by the **Sustained Uplink Data Rate** and **Sustained Downlink Data Rate** variable fields in the AP.

Recharging Buckets

The **Uplink Burst Allocation** and **Downlink Burst Allocation** variable fields in the AP set the size of each bucket. This limits the maximum number of tokens that can fill a bucket.

If the SM transfers data at the Sustained Data Rate, then the bucket refills at the same rate, and burst is impossible. If the SM transfers data at a rate less than the Sustained Data Rate, then the bucket continues to fill with unused tokens. In this case, required bursting occurs up to the number of unused tokens.

After a burst is completed, the bucket is recharged at the Sustained Data Rate. Short bursts recharge faster than large bursts.

4.1.2 Bandwidth from the SM Perspective

Normal web browsing, e-mail, small file transfers, and short streaming video are rarely rate limited, depending on the bandwidth management (QoS) settings in the AP or the BAM server. When the SM processes large downloads such as software upgrades and long streaming video, or a series of medium-size downloads, these transfer at a bandwidth higher than the Sustained Date Rate (unless no unused tokens remain in the bucket) until the burst limit is reached.

When the burst limit is reached, the data rate falls to the Sustained Data Rate setting. Then later, when the SM is either idle or transferring data at a rate slower than Sustained Data Rate, the burst limit recharges at the Sustained Data Rate.

4.1.3 Interaction of Burst Allocation and Sustained Data Rate Settings

In the scenario shown in Figure 3, the Burst Allocation is set to 1200 kb and the Sustained Data Rate is set to 128 kbps. The large data burst in this illustration is transmitted without delay because the Burst Allocation is set high enough. After the burst, the bucket experiences a significant recharge. A small burst and then a quick recharge follow before transmission at the Sustained Data Rate resumes.

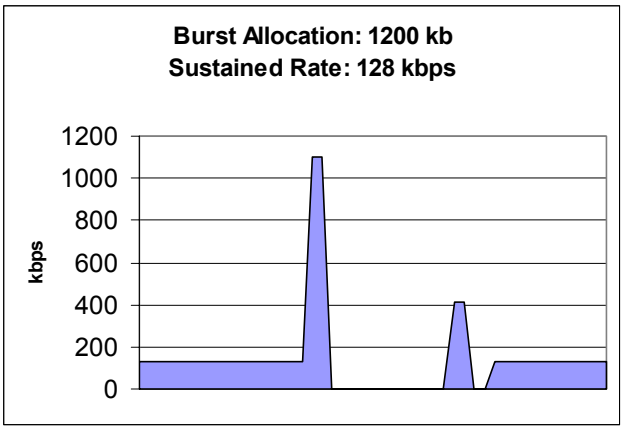


Figure 3: Greater Burst Allocation value

In the scenario shown in Figure 4, the Burst Allocation is set to 128 kb and the Sustained Data Rate is set to 128 kbps. Even when the transmission rate occasionally decreases in this illustration, a burst is unnecessarily limited to the low Burst Allocation value. This configuration cancels the advantage of a settable Burst Allocation.

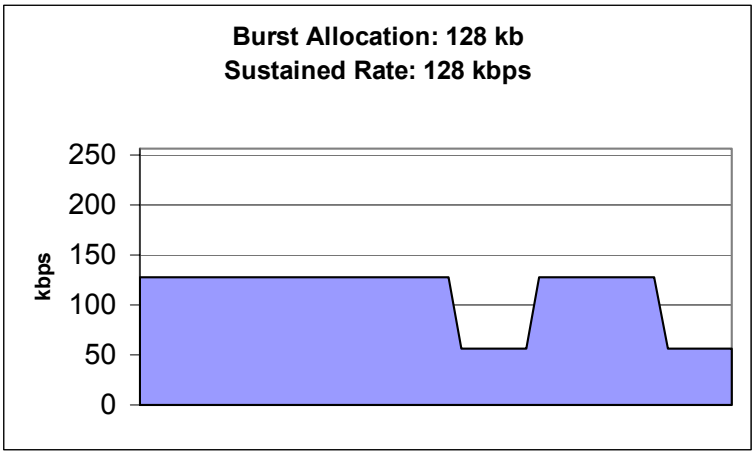


Figure 4: Equal Burst Allocation value

4.1.4 Examples of Tiered Service Levels for SMs

Examples of levels of service that vary by bandwidth capability are provided in Table 5.

> ***NOTE:*** The service times that Table 5 correlates to service levels are best case. These do not account for transient limitations such as congestion on the Internet or for network configuration limitations such as server-side bandwidth capability.

Table 5: Examples of SM tiers

Rate	Basic Service	Enhanced Service	Premium Service
Sustained Uplink and Sustained Downlink Data Rates	128 kbps	512 kbps	No restrictions
Uplink Burst and Downlink Burst Allocations	40,000 kb (5 MB)	80,000 kb (10 MB)	No restrictions
Initial burst speed	2.5 Mbps	2.5 Mbps	2.5 Mbps
Time to download medium complexity web page	1 sec	1 sec	1 sec
Time to download 5 MB	16 sec	16 sec	16 sec
Time to download 10 MB	336 sec	32 sec	32 sec
Time to download 25 MB	1296 sec (over 20 min)	272 sec	80 sec

4.2 AUTHENTICATION

This section describes the message exchanges that support authentication between network elements and the log that maintains a record of the latest authentication event.

4.2.1 Authentication Process

When an SM attempts to register to an AP that the operator has set to require authentication

1. An SM attempts registration to an AP.
2. The AP calls the BAM server to report that an SM is attempting to register but must be authenticated and to derive the bandwidth configuration to apply to the SM.

   NOTE: Messages that are exchanged in the following sequence are recorded on the BAM server in the `/var/log/canopy/canopy.log` file. However, the BAM server does not display these messages.
3. The active BAM server checks its list of correlated APs and licenses. See License Forfeiture and Reassignment on Page 17.

   If the BAM server finds a license currently correlated to the AP (the AP has responded to all ping attempts since the correlated license was assigned), then the BAM server returns to the AP a challenge with random number (as illustrated in Figure 5).

   If the BAM server finds that no license is currently correlated to the AP, then the BAM server calls the license server(s).

   - If the majority of license servers find that no AP floating license remains unassigned, then
     a. the license servers inform the BAM server that the request *has not* been processed.
     b. the BAM server responds to the AP that the request cannot be processed.
   - If the majority of license servers recognize that an unassigned AP floating license exists, then
     a. the license servers process the request and inform the BAM server that the license request has been processed.
     b. the BAM server correlates the newly assigned license to the AP.
     c. the BAM server returns to the AP a challenge with random number (as illustrated in Figure 5).

   NOTE: When a license server is out of service, no new licenses are assigned but previously assigned licenses remain effective.

From this point, the message flow between the network elements is as illustrated in Figure 5.

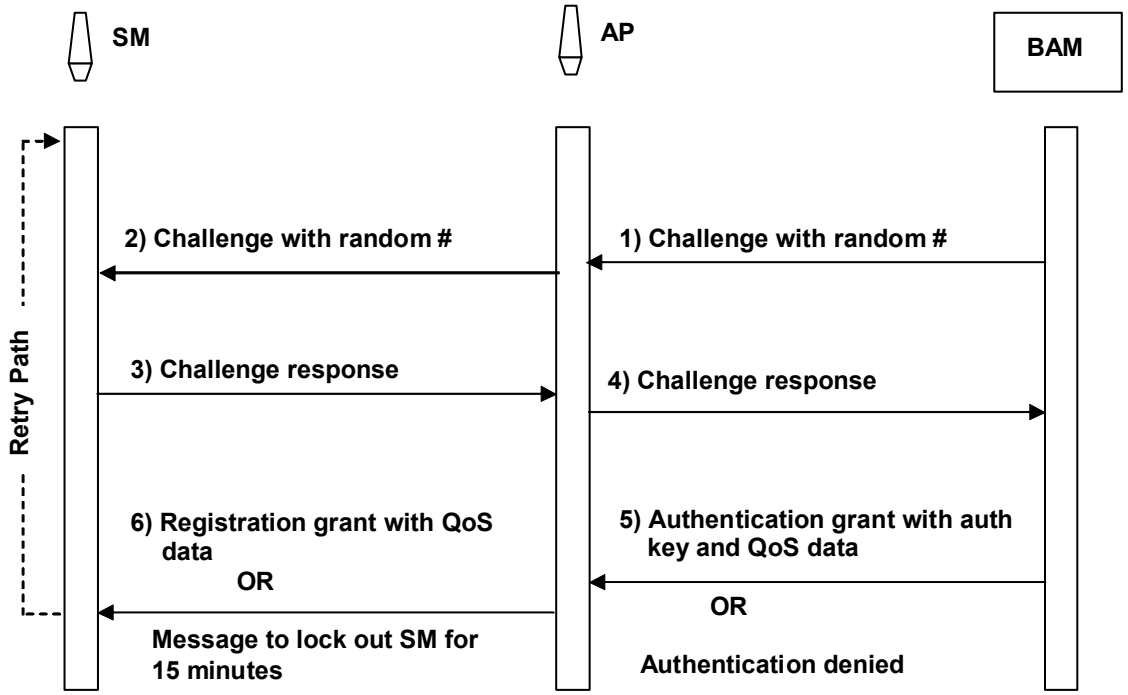


Figure 5: Authentication message flow

The processing of these messages is as follows:

1. BAM generates a random number and sends this number in a challenge to the AP.
2. The AP passes the challenge to the SM.
3. The SM uses either a factory-set key or the operator-assigned key (from the SM Configuration page) to calculate a response to the challenge, then sends this response to the AP.
4. The AP passes the challenge response to the BAM server.
5. BAM evaluates the challenge response against the authentication key in the BAM SQL database. This key correlates to the original random number. BAM allows or denies service as follows:
   - If the SM correctly responded to the challenge, then
     - the BAM server sends through the AP a message that authenticates the SM and provides QoS information that the AP and SM use and store.
     - the AP allows the SM onto the network.
   - If the SM either incorrectly responded to the challenge or is absent from the BAM SQL database, then
     - the BAM server sends to the AP a message that denies authentication for the SM.
     - the AP sends to the SM a message that prevents authentication attempts for the next 15 minutes.

4.2.2 Keys and Random Number

Beyond the floating license keys for BAM server(s) and APs, three keys and a random number are involved in authentication as follows:

- factory-set key in each SM. Neither the subscriber nor the network operator can view or change this key.
- authentication key, also known as *authorization key* and *skey*. The network operator sets this key both in the Configuration page of the SM and in the ESN database. In the **Authorization key** parameter of the SM Configuration web page, password access to the page governs whether the network operator or the subscriber can view and set this key.
- random number, generated by BAM and used in each attempt by an SM to register and authenticate. Neither the subscriber nor the network operator can view this number.
- session key, calculated separately by the SM and BAM, based on both the authentication key (or, by default, the factory-set key) and the random number. BAM sends the session key to the AP. Neither the subscriber nor the network operator can view this key.

None of the above keys is ever sent in an over-the-air link during an SM registration attempt. However, with the assumed security risk, the operator can create and configure an authentication key in the Authentication Key field of the SM Configuration page. See Configuration in the AP and SM on Page 44.

4.2.3 Log of Authentication Events

Whenever BAM authenticates or denies authentication to an SM, BAM records the time, date, and final status of this transaction into the SQL database. This record overwrites data from the previous authentication transaction.

NOTE: Where the database is maintained on a RADIUS server, the BAM server acts as only a proxy server and *does not* perform authentication or write a record of the transaction into the database.

4.3 SQL DATABASE

Where the database *is not* maintained on a RADIUS server, the SQL database maintains records for each SM, keyed by the ESN (electronic serial number or MAC address) of the SM. These records identify the authentication key and contain QoS information.

> ***NOTE:*** For systems where multiple SQL databases exist (on multiple servers), the `ESN`, `Secret Key`, and `QOS` fields must be identically stored in each database to ensure that BAM can properly handle the next authentication attempt from the SM.

4.3.1 ESN Data Table

The input to the MySQL or PostgreSQL database is an ESN Data Table, in which each row represents one SM. In tab-separated fields, each row stores the ESN, authentication Key, and QoS information that apply to the SM. These fields are defined in Table 6.

Table 6: Definition of ESN Data Table fields

Field	Format	Notes
ESN	12 hexadecimal characters (including `0` to `9` and `a` to `f`)	The MAC address of the SM. Shown as "Device type" on the SM web-accessed Status page. Shown as the 12 character serial number labeled S/N under FCC ID when you pop the base cover off the SM. Not the same as the 10 character hardware serial number labeled S/N on the outside of the SM.
Authentication Key	32 hexadecimal characters (including `0` to `9` and `a` to `f`)	All 0s defaults to the use of the factory-set key. Authentication keys should be random or pseudo-random, and per SM (must match the SM and is, therefore, not the same for multiple SMs.)
QoS	64 hexadecimal characters (including `0` to `9` and `a` to `f`) in 5 contiguous subfields	Subfield formatting is as follows: Subfield 1: Sustained uplink data rate, in kilobits per second, converted to hex, 4 characters. Subfield 2: Sustained downlink data rate, in kilobits per second, converted to hex, 4 characters. Subfield 3: Uplink burst size, in kilobits converted to hex, 8 characters. Subfield 4: Downlink burst size, in kilobits converted to hex, 8 characters. Subfield 5: Unused, 40 characters

Examples of a data from a typical ESN Data Table are displayed in Figure 6, Figure 7, and Figure 8.

```
0a003e002037 12345678901234567890123456789012   0080008000000a0000000a000000000000000000000000000000000000000000
0a003e002038 ab2396cd19ebf19ab294827f6efb1928   0200020000000b0000000b000000000000000000000000000000000000000000
0a003e002039 1290cde76fa63e384cb0d9a83e8b8c38   0400040000000c0000000c000000000000000000000000000000000000000000
```

Figure 6: Typical ESN Data Table, Columns 1, 2, and 3

```
0a003e002037 12345678901234567890123456789012
0a003e002038 ab2396cd19ebf19ab294827f6efb1928
0a003e002039 1290cde76fa63e384cb0d9a83e8b8c38
```

Figure 7: Typical ESN Data Table, Columns 1 and 2

```
0080008000000a0000000a000000000000000000000000000000000000000000
0200020000000b0000000b000000000000000000000000000000000000000000
0400040000000c0000000c000000000000000000000000000000000000000000
```

Figure 8: Typical ESN Data Table, Column 3

4.3.2 Canopy Data Formatter (CDF) Script for ESN Data Table Creation

For the GUI import operation (not for the command **`config upload database`** SSE command line interface), the BAM distribution includes a Canopy Data Formatter (CDF) script that creates an initial ESN Data Table. This script converts decimal to hexadecimal and pads the fields with trailing zeros.

4.3.3 Relationship of ESN Data Table, XML Data File, and SM Database

The relationship of files and databases is displayed in Figure 9 and Figure 10.

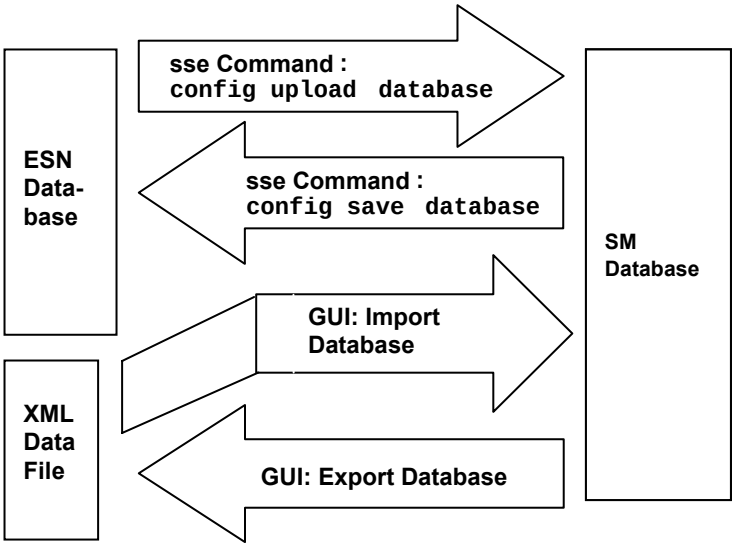


Figure 9: Database inputs and outputs without cdf script

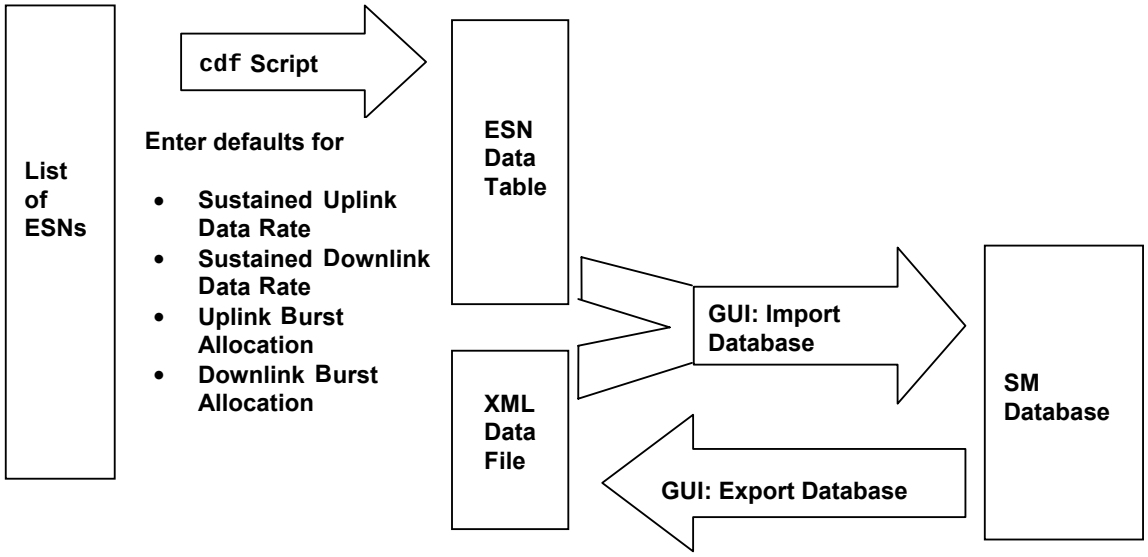


Figure 10: Database inputs and outputs with cdf script

5 INSTALLATION AND OPERATION PROCEDURES

5.1 INSTALLATIONS AND TESTS

5.1.1 Acquire the Initial Software

Canopy distributes BAM Release 2.0 software to customers who previously purchased either BAM Release 1.0 or 1.1. All other customers and those who wish to extend their BAM coverage to additional BAM servers and APs should order the needed software and licenses. The distribution of BAM software and license keys for LM server(s), BAM server(s), and APs is described under Software and License Distribution on Page 9.

To acquire Red Hat Enterprise Linux (ES or WS) Version 3 operating system, visit http://www.redhat.com/software/rhel.

5.1.2 Plan the Installations

Since the hard drives of each previously deployed BAM server and database server must be reformatted before Red Hat Enterprise Linux Version 3 is installed, examine the file systems that you have on those servers. Identify all essential files, including the current ESN data file, to copy to an alternate medium before the installation.

During the operating system and application installations and tests, the server will be unavailable to perform authentication. You should allow at least a 2-hour block of time for installations and tests. However, as in other installations, the speed of the server(s) affects the amount of time required.

In this interval, SMs that are currently required to authenticate will be denied service if either

- no BAM server listed in the AP is operating
- the database server that the BAM server calls for data about the SM is not operating.

To prevent this, identify the IP address of each AP on which the authentication mode should be disabled during the installations. A procedure for disabling the authentication mode is provided under Disable Authentication in Affected APs on Page 33.

During your Red Hat Enterprise Linux Version 3 installation, you will need to call the Red Hat network web site to acquire additional software, which is unavailable at the earlier stage. Ensure that each server has Internet access during this installation.

5.1.3 Copy Essential Files to Alternate Media

If you are upgrading BAM from Release 1.0 to Release 2.0, save a copy of the ESN Data as shown in Figure 11. This data can then be used after the upgrade of Linux and BAM software.

IMPORTANT: Do not use this procedure if you are upgrading BAM from Release 1.1.

Distinctive fonts indicate

literal user input.
variable user input.
literal system responses.

```
$ telnet localhost 9080

CanopySSE:>config save table /mnt/floppy/canopydata  (or other target)
config save table /mnt/floppy/canopydata
OK
CanopySSE:>exit
exit
Connection closed by foreign host.
```

Figure 11: Example session to preserve ESN Data Table

If you are upgrading BAM from Release 1.1, perform the following steps:

1. Open a browser window.
2. If your browser is directly connected to the BAM server, access the site http:///*localhost*/gui.

   If your browser *is not* directly connected to the BAM server, enter the IP address that identifies the BAM server as *localhost*. (Access to the BAM GUI is possible from any network element that can access the BAM server by IP address.)
   RESULT: the BAM server presents the BAM GUI (graphical user interface).
3. Select **Subscriber Configuration**.
4. Select **Subscriber Configuration Login**.
5. Select **Export Database**.
6. Select **Download**.
7. Ensure that **Save this file to disk** is selected.
8. Click **OK**.
9. Browse to the target location for the backup copy.
10. Enter a file name for the backup copy.
11. Click **Save**.

Save all other essential files from both the database server and the BAM server to alternate media.

5.1.4 Disable Authentication in Affected APs

To disable authentication in the APs that will be unable to authenticate SMs during the installations, *either*

1. Download the Canopy Network Updater Tool and supporting documentation from http://motorola.canopywireless.com/softwareupdates/fileinfo.php?catid=4.
2. Download the AP Authentication tool and supporting documentation.
3. Launch the Canopy Network Updater Tool.
4. Select the APs you identified under Plan the Installations on Page 31.
5. Execute the AP Authentication Control external tool.

or

1. Visit the Configuration web page of each of these APs
2. Change the value of the **Authentication Mode** parameter to either **Authentication Optional** or **Authentication Not Required**.
3. Click **Save Changes**.
4. When prepared to commit these changes, click **Reboot**.

5.1.5 Install Red Hat Enterprise Linux Version 3

NOTE: The database server may exist on the same computer as BAM.

On each server whose operating system will be replaced, ensure that you have copied all essential files, including ESN data, onto alternate media. Then format the hard drive(s).

Begin the Red Hat Enterprise Linux Version 3 Installation

No upgrade path exists from Red Hat Linux 9 to Red Hat Enterprise Linux Version 3. Thus, to install Enterprise Linux Version 3, which is required for BAM Release 2.0, you must take the BAM server off line. Where a redundant BAM server is deployed, authentication requests continue to be processed while you install Enterprise Version 3 onto the original primary BAM server. Where no redundant BAM server is deployed, taking the only BAM server offline disables authentication services and results in SMs being denied service by any AP that is set to require authentication. To prevent SMs being denied service, first either

- disable authentication in the Configuration page of each AP that is associated with the BAM server.
- use the AP Authentication Control external tool to disable authentication on all APs in a single execution.

Download the installation procedure for Red Hat Enterprise Linux Version 3 (WS or ES) from http://www.redhat.com/docs/manuals/enterprise/. Begin the installation as follows:

1. Format the hard drive.
2. Change the radio button from **Accept the current package** to **Customize the set of package to be installed**.
3. Select **Web Server**.
4. Click the **Details** button.
5. To support a MySQL database, select **php-mysql-4.3.2-11.ent**.
6. Select **php-odbc**.

7. To support a PostgreSQL database, select **php-pgsql-4.3.2-11.ent**.
8. Select **ODBC driver**.
9. To support a PostgreSQL database, perform the following steps:
   a. From under **Server**, select **SQL Database**.
   b. Click the **Details** button.
   c. Select drivers **rh-postgresql**, **rh-postgresql-contrib**, and **rh-postgresql-docs**.
   d. Select **postgres-odbc-7.3-3**.
   e. Ensure that the **unixODBC-2.2.8-2.3.0.2** package is selected.
10. To support a MySQL database, perform the following steps:
    a. From under **Server**, select **MySQL Database**.
    b. Click the **Details** button.
    c. Select **php-mysql-4.3.2-11**.
    d. Ensure that the **unixODBC-2.2.8-2.3.0.2** package is selected.

NOTE: At this point in the installation, the Mozilla browser is available for web access to additional files that you will need.

Register Red Hat

Visit http://www.redhat.com/software/rhel/register/ and follow registration instructions.

Acquire Remaining Software

To acquire the remaining software, perform the following steps:

1. Visit http://rhn.redhat.com.
2. Click on **RHN LOGIN**.
3. Log in.
4. To support a PostgreSQL database, download the **rh-postgresql-server-7.3.6-1** rpm package.
5. To support a MySQL database, download the **mysql-server-3.23.58-1** rpm package.

Install the Server Software

To support a PostgreSQL database, as `root`, enter
`rpm -ivh rh-postgresql-server-7.3.6-1.rpm`.

RESULT: The following server packages are installed on the BAM server:

rh-postgresql-docs-7.3.6-1

php-pgsql-4.3.2-11.ent

rh-postgresql-contrib-7.3.6-1

rh-postgresql-server-7.3.6-1

rh-postgresql-libs-7.3.6-1

rh-postgresql-7.3.6-1

Where the database resides on a different server from BAM, copy and install the file **rh-postgresql-server-7.3.6-1** (installed above) onto the database server.

To support a MySQL database, as `root`, enter
`rpm -ivh mysql-server-3.23.58-1.rpm`.

RESULT: The following server packages are copied to the BAM server:

mysql-server-3.23.58-1

php-mysql-4.3.2-11.ent

mysql-3.23.58-1

Where the database resides on a different server from BAM, copy and install the file **mysql-server-3.23.58-1** (installed above) onto the database server.

5.1.6 Set up ODBC

To set up the ODBC driver for a PostgreSQL database, perform the procedures that are provided under

- Set up BAM GUI for PostgreSQL Database on Page 46
- Test the ODBC Driver for PostgreSQL on Page 48

To set up the ODBC driver for a MySQL database, perform the procedures that are provided under

- Set up BAM GUI for MySQL Database on Page 55
- Test the ODBC Driver for MySQL on Page 57

5.1.7 Set Up License Management

See *Canopy Networks License Manager User Guide.*

Install FLEXnet Licensing Software

See Canopy Networks License Manager User Guide.

Install Licenses

See *Canopy Networks License Manager User Guide.*

5.1.8 Set Up BAM

Copy BAM Release 2.0 to the BAM Server

Copy the files from the BAM Release 2.0 distribution CD-ROM to a directory on the BAM server as follows.

Distinctive fonts indicate

`literal user input.`
`variable user input.`
`literal system responses.`

1. Enter **`mkdir BAM2.0`**
2. Enter **`cd BAM2.0`**

3. Enter **`cp /mnt/cdrom/* .`**
   RESULT: All of the BAM Release 2.0 files are copied to the server.

Install the BAM Database

The BAM database must be installed before BAM Release 2.0. However, this *is not* the case where a RADIUS database will be used.

1. If you will implement a PostgreSQL database, perform the following required steps:
   a. Log in as `root`.
   b. Enter **`su postgres`**.
   c. Enter **`createuser root`**.
   d. At the prompt
      `Shall the new user be allowed to create databases? (y/n)`,
      select **`Yes`**.
   e. At the prompt
      `Shall the new user be allowed to create more new users? (y/n)`,
      select **`Yes`**.
   f. Enter **`createdb root`**.
2. To optionally view how to use the installation utility, in the directory created above, enter **`./installdb –help`**.
3. In the same directory, enter one of the following commands:
   `./installdb Postgres` (to use a PostgreSQL database)
   `./installdb MySQL` (to use a MySQL database)

Install BAM Release 2.0

Install BAM Release 2.0 software as follows.

Distinctive fonts indicate

`literal user input.`
`literal system responses.`

1. To optionally view how to use the installation utility, in the same directory, enter **`./installbam –help`**.
2. In the same directory, enter one of the following commands:
   `./installbam Postgres` (to use a PostgreSQL database)
   `./installbam MySQL` (to use a MySQL database)
   `./installbam Radius` (to use a RADIUS database)

   RESULT: The system displays license terms and conditions.

   NOTE: As you read the displayed response, if you press the Enter key, the display advances (scrolls) a single line. If you press the spacebar, the display advances an entire screen.
3. If you agree with the terms of the displayed license terms and conditions, enter **`1`**.
   RESULT: The system competes the installation and responds: `Software installation is complete.`

Verify BAM Release 2.0 Installation

Perform the following steps to verify that the installation of BAM Release 2.0 software was successful:

> Distinctive fonts indicate
>
> **`literal user input.`**
> `literal system responses.`
> *`variable`* `system responses.`

1. Enter **`/etc/rc.d/init.d/engined status`**
   RESULT: The system responds `engined (pid` *`PID`*`) is running`.
2. Enter **`/etc/rc.d/init.d/ssed status`**
   RESULT: The system responds `ssed (pid` *`PID`*`) is running`.
3. If the system fails to return the above responses
   a. repeat the installation as described under Install BAM Release 2.0 on Page 36.
   b. repeat the verification steps as described in this procedure.
4. Enter **`exit`** (to exit as `root` from the command-line interface).

Administer Access and Accounts

To administer the access and accounts on the BAM server, perform the following steps:

1. Boot the server(s).
2. Open a browser window.
3. If your browser is directly connected to the BAM server, access the site http:///*localhost*/gui.

If your browser is on the BAM server, enter the IP address that identifies the BAM server instead of *localhost*. (Access to the BAM GUI is possible from any network element that can access the BAM server by IP address.)
RESULT: the BAM server presents the BAM GUI (graphical user interface).

If any required package was omitted from the installation, then the SQL database will not be accessible and the GUI will display the following errors:

Unable to authenticate Administrator.
Please check your user name and/or password.
DB Error: no such address.

IMPORTANT: In any BAM GUI session, to return to a previously loaded BAM web page, use the **back** button in the GUI rather than the Back button of your browser. Using the browser Back button causes the session to lose some settings and generate errors.

4. Select **Administration**.
5. Select **Administrator Login**.
   NOTE: The Administrator password is the database software `root` user password, which is initially blank.
6. Select the database server.

7. If you wish to continue to leave this password blank for the present GUI session, click **Log In**.

   If you wish to reset this password to other than blank, then

   a. Access the shell on the BAM server.

   b. Enter **`mysqladmin -u root password yourpassword`**
   or **`psql -U canopy --command "ALTER USER canopy PASSWORD 'yourpassword'"`**

   c. Exit from the shell.

   d. Return to the GUI session.

   e. Enter the syntax of ***`yourpassword`*** into the Administrator password field.

   f. Click **Log In**.

7. Click the **Click here for Canopy Administration Options** link.
   RESULT: The Canopy User Administration interface page opens.
8. Click **Add**.
9. Enter a user name and password.
10. Select an associated user access level (**Read-Write** or **Read-Only**).
11. Click **Add User**.
12. If you wish to specify an additional user

    a. click **back**.

    b. repeat Steps 8, 9, and 10.

    If you do not wish to specify an additional user, click **Log Off**.

Import or Generate the ESN Data

To import an ESN Data Table, perform the following steps:

1. Note the path to the desired ESN Data Table file. This file may have been
   - generated by a `cdf` script.
   - saved from another BAM server with which you want to synchronize this server.
2. Open a browser window.
3. If your browser is directly connected to the BAM server, access the site http:///*localhost*/gui.

   If your browser *is not* directly connected to the BAM server, enter the IP address that identifies the BAM server as *localhost*. (Access to the BAM GUI is possible from any network element that can access the BAM server by IP address.)
   RESULT: the BAM server presents the BAM GUI (graphical user interface).

   IMPORTANT: In any BAM GUI session, to return to a previously loaded BAM web page, use the **back** button in the GUI rather than the Back button of your browser. Using the browser Back button causes the session to lose some settings and generate errors.
4. Select **Subscriber Configuration**.
5. Select **Subscriber Configuration Login**.
6. Enter your user name and password.
7. Click **Log In**.

8. Click the **Click here for Configuration Options** link.
9. From the left sidebar frame menu, select **Import Database**.
10. In the **Upload Import File** field, either
    a. leave the default selection selected to only recover SMs from the last previous backup.
    b. browse to, or enter the path of, the ESN Data Table file that was noted in Step 1.
11. Select **Upload File**.
    RESULT: The GUI screen displays the successfully imported ESN Data Table.

To generate a new ESN Data Table, perform the following steps.

NOTE: The ESN data file that this procedure generates can be used for the GUI import operation (not for the command **`config upload database`** SSE command line interface).

Distinctive fonts indicate

`literal user input.`
`variable` **`user input.`**

1. Optionally, enter **`./cdf`** to preview instructions for the `cdf` command-line script.
   NOTE: Table 7 defines the values that should be substituted for the variables in Step 2.

Table 7: Definitions of cdf script variables

Variable	Definition
`infile.txt`	Path to the file that contains a list of ESNs, one ESN per line, and with hyphens separating each pair of characters.
`outfile.txt`	Path to the output file, which will contain the initial ESN Data Table.
`suldr`	An initial default value for the **Sustained Uplink Data Rate** parameter.
`sdldr`	An initial default value for the **Sustained Downlink Data Rate** parameter.
`ulba`	An initial default value for the **Uplink Burst Allocation** parameter.
`dlba`	An initial default value for the **Downlink Burst Allocation** parameter.
NOTE: See Interaction of Burst Allocation and Sustained Data Rate Settings on Page 23.	

2. Enter **`.cdf infile.txt outfile.txt suldr sdldr ulba dlba`**
   RESULT: The GUI uses the contents of *`outfile.txt`* as the default ESN Data Table if the operator imports this file as described under Import or Generate the ESN Data on Page 38. The command-line interface uses the contents of *`outfile.txt`* as the default ESN Data Table when the command **`config upload table outfile.txt`** is entered, as described under SSE Database Commands on Page 63.
3. Enter **`exit`** (to leave the command-line interface).

Re-enable Authentication in Affected APs

To re-enable authentication in the APs, perform the following steps:

1. Put an SM within radio reach of one of the APs you identified under Plan the Installations on Page 31.
2. Access the Configuration web page of the AP.
3. Set the **Authentication Mode** parameter to **Authentication Enabled**.
4. Attempt to register the SM to the AP.
5. Launch the Canopy Network Updater Tool.
6. Select the APs.
7. Execute the AP Authentication Control external tool.

5.2 MANAGEMENT OF QOS AND AUTHENTICATION

Use the following procedures to manage authentication and bandwidth data about the SMs.

- Use the GUI to Change Subscriber Data (as described on Page 40).
- Use the GUI to Suspend or Reinstate Service to a Subscriber (as described on Page 41).
- Use the GUI to Back Up an ESN Data Table (as described on Page 42).
- Customize the GUI (as described on Page 43).
- Use the Command-line Interface to Change SM QoS Data (as described on Page 43).

IMPORTANT: In any BAM GUI session, to return to a previously loaded BAM web page, use the **back** button in the GUI rather than the Back button of your browser. Using the browser Back button causes the session to lose some settings and generate errors.

5.2.1 Use the GUI to Change Subscriber Data

To change subscriber data, perform the following steps:

1. Open a browser window.
2. If your browser is directly connected to the BAM server, access the site http://*localhost*/gui.

   If your browser *is not* directly connected to the BAM server, enter the IP address that identifies the BAM server as *localhost*. (Access to the BAM GUI is possible from any network element that can access the BAM server by IP address.)
   RESULT: the BAM server presents the BAM GUI (graphical user interface).
3. Select **Subscriber Configuration**.
4. Select **Subscriber Configuration Login**.

5. Select **Subscriber Administration**.
6. Optionally, click the **Search** button and enter either part or all of the ESN of the SM.
7. In the **Select** column, click the box that corresponds to the SM whose data you wish to change.
   NOTE: In the following step, selection of **Modify** allows you to change any parameter (data in any column of the row), except the ESN.
8. Select **Add**, **Modify**, or **Delete**.
9. If you selected **Modify** in Step 8, modify the SM configuration as desired.
   If you selected **Add** in Step 8, enter the ESN and all parameters as desired.
10. Click **OK**.
11. For any other SM whose data you wish to change, repeat Steps 7 through 10.
    RESULT: The BAM server applies the QoS data changes upon the next registration of the SM (not immediately for an SM that is registered when the changes are made).

5.2.2 Use the GUI to Suspend or Reinstate Service to a Subscriber

In BAM Release 2.0 or later, you can use the BAM GUI to indefinitely suspend service to a subscriber without dropping the BAM data that has applied to that subscriber. Then at a later time, since the bandwidth configuration is retained in the database, you can use the BAM GUI to reinstate service to that subscriber without reconfiguring the authentication and bandwidth assigned to that subscriber. The **Account** column in the BAM GUI provides the **Active** and **Suspend** selections, as shown in Figure 12.

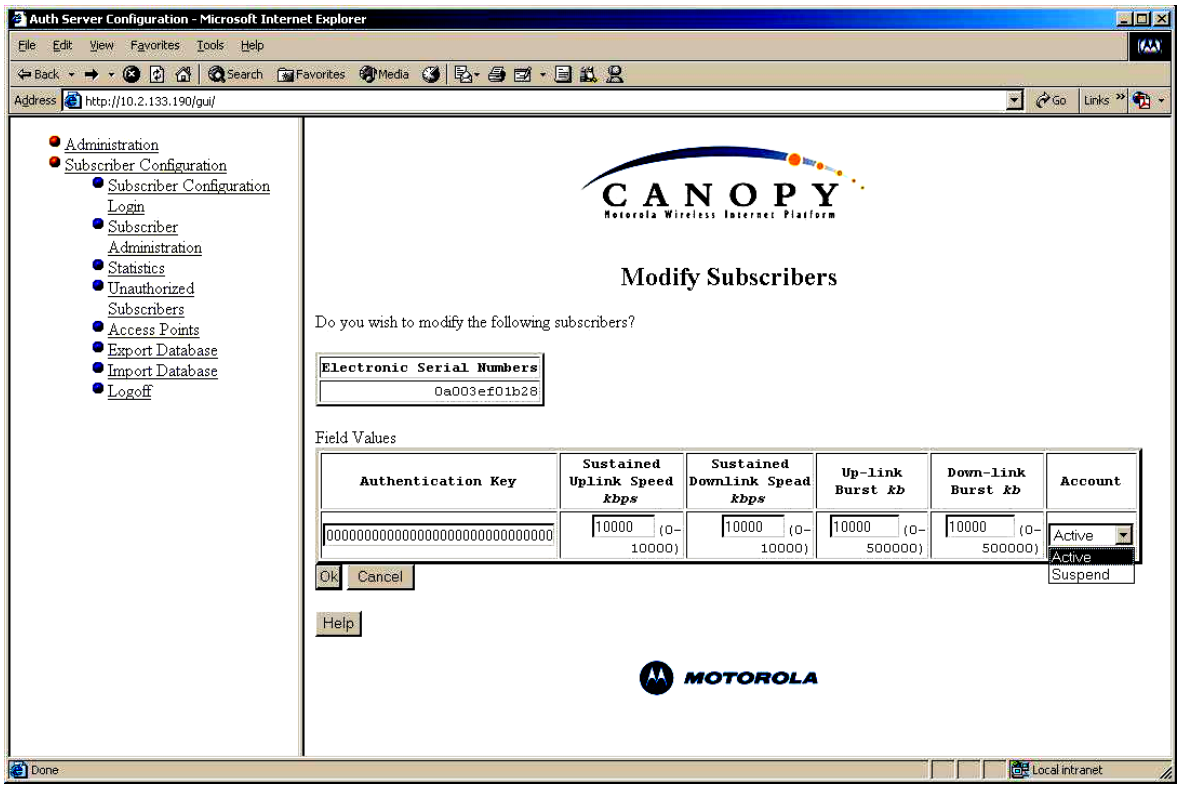


Figure 12: Activating or suspending access for the subscriber

After you select **Active** or **Suspend** in the **Account** column, click the **Ok** button. The system responds that the record has been updated and displays the new value, as shown in Figure 13.

IMPORTANT: In any BAM GUI session, to return to a previously loaded BAM web page, use the **back** button in the GUI rather than the Back button of your browser. Using the browser Back button causes the session to lose some settings and generate errors.

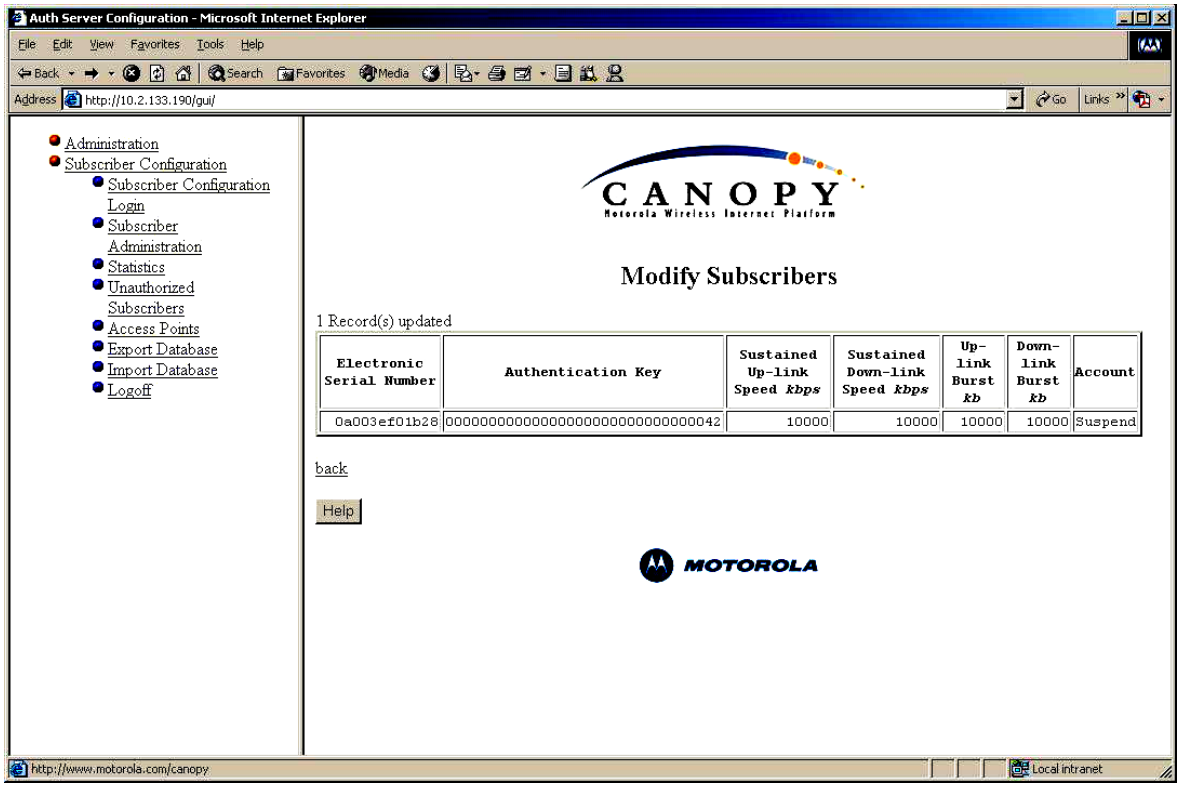


Figure 13: Access suspended for the subscriber

NOTE: When you suspend access by using the BAM SSE CLI, access is immediately suspended for the subscriber (a current session is dropped). By contrast, when you suspend access by using the BAM GUI, access is not suspended until the next registration attempt from the subscriber.

5.2.3 Use the GUI to Back Up an ESN Data Table

To optionally back up the ESN Data Table file through the GUI, perform the following steps:

1. Open a browser window.
2. If your browser is directly connected to the BAM server, access the site http://*localhost*/gui.

   If your browser *is not* directly connected to the BAM server, enter the IP address that identifies the BAM server as *localhost*. (Access to the BAM GUI is possible from any network element that can access the BAM server by IP address.)
   RESULT: the BAM server presents the BAM GUI (graphical user interface).
3. Select Subscriber Configuration.

4. Select Subscriber Configuration Login.
5. Select Export Database.
6. Select Download.
7. Ensure that **Save this file to disk** is selected.
8. Click **OK**.
9. Browse to the target location for the backup copy.
10. Enter a file name for the backup copy.
11. Click **Save**.

5.2.4 Customize the GUI

Optionally, you can customize the GUI through either or both of the following procedures.

To change the number of rows of data that the GUI displays per page, perform the following steps:

1. Enter **su -** to log in as `root`.
   NOTE: Use your editor utility for Steps 2 through 6.
2. Open the file `/usr/local/canopy/include/canopy.xml`
3. Find the line `<row size="N" />`, where *N* is a number.
4. Change the value of ***N*** to the desired point size of data that the GUI displays. (A smaller number causes more rows of data to be displayed.)
5. Save the file (`/usr/local/canopy/include/canopy.xml`).
6. Close the file.
7. Click **Subscriber Configuration Logoff**.
8. Click **Subscriber Configuration Login**.

To add a new database to the GUI **Database Server** pull-down menu, perform the following steps:

1. Enter **su -** to log in as `root`.
   NOTE: Use your editor utility for Steps 2 through 6.
2. Open the file `/usr/local/canopy/include/canopy.xml`.
3. Duplicate the tag `<database host="localhost" />`.
4. In the duplicate tag, replace `localhost` with the address of the new database.
5. Save the file (`/usr/local/canopy/include/canopy.xml`).
6. Close the file.
7. Click **Subscriber Configuration Logoff**.
8. Click **Subscriber Configuration Login**.
   RESULT: The new database is added to the menu.

5.2.5 Use the Command-line Interface to Change SM QoS Data

To create and delete subscriber QoS data through the command-line interface, use the commands that are described under SSE Database Commands on Page 63.

5.3 CONFIGURATION IN THE AP AND SM

For each AP and SM that will use BAM to manage authentication and bandwidth, perform the following steps:

1. Launch a browser.
2. Access the Configuration page of the AP.
3. In the **Airlink Security** parameter, select **Encryption Disabled** or **Encryption Enabled**, as appropriate.
   NOTE: An early software release may instead provide a **DES Enhanced & Authentication Required** selection.
4. Click the **Save Changes** button.
5. Click the **Reboot** button.
6. In the **Authentication Mode** parameter, select either **Authentication Enabled** or **Authentication Optional**.
   NOTE: An early software release may instead provide a **Use Authentication if Available** selection.
7. In the **Authentication Server IPs** parameter, enter the IP addresses of one, two, or three BAM servers.
   NOTE: Populate these in order of primary, secondary, and tertiary. For any unused server position, enter 0.0.0.0.
8. Click the **Save Changes** button.
9. Click the **Reboot** button.
10. In the BAM GUI, select **Access Points** from the selections on the left side of the web page.
11. For each **Access Point Alias**, define a *unique* string as the alias of the AP.
    NOTE: This is a recommendation.
12. Access the Configuration page of the SM.
13. In the **Authentication Key** parameter, select **Use Default Key**.
14. Click the **Save Changes** button.
15. Click the **Reboot** button.
16. Exit the browser.

6 HISTORY OF CHANGES IN THIS DOCUMENT

Issue 4 introduced the following changes:

- Editorial changes to reduce redundancy and clarify technical concepts
- New information on how Burst and Sustained Data settings interact. See Interaction of Burst Allocation and Sustained Data Rate Settings on Page 23.

Issue 3 introduced the following changes:

- BAM Release 1.1—Graphical User Interface

Issue 2 introduced the following changes:

- Script for installing MySQL and BAM software
- Software license agreement in script

APPENDIX 1: PostgreSQL DATABASE SUPPORT

SET UP BAM GUI FOR PostgreSQL DATABASE

NOTE: The following procedure presumes that **unixODBC-2.2.8-2.3.0.2**, the database client, and the ODBC driver (**postgres-odbc**) have been installed. If any package was incorrectly omitted or selected, you can use the add or remove function from the system menu to select or omit the package.

Distinctive fonts indicate

literal user input.
variable user input.
literal system responses.
variable system responses.

To set up a system-wide ODBC driver to use a PostgreSQL database, perform the following steps on the client computer:

1. On the computer where engined/ssed will run, enter **su -** to log in as `root`.
2. Change directory to `/usr/local/etc/`.
3. Open or create the file `odbcinst.ini`.
4. Add the following lines to the file:

```
[PostgreSQL]
Description=PostgreSQL driver for Linux
Driver=/usr/lib/psqlodbc.so
FileUsage=1
```

5. Save and close the file `odbcinst.ini`.
6. Enter **odbcinst -I -d -f /usr/local/etc/odbcinst.ini**.
   RESULT: The ODBC driver is installed.
7. In the same directory (`/usr/local/etc/`), open or create the file `odbc.ini`.
8. Add the following lines to the file:

```
[psql]
Description=PostgreSQL to connect to canopy
Driver=PostgreSQL
Trace=Yes
TraceFile=/tmp/sql.log
Database=canopy
Servername=localhost  (This can be a remote server)
UserName=canopy
Port=
Protocol=6.4
ReadOnly=No
RowVersioning=No
ShowSystemTables=No
ShowOidColumn=No
FakeOidIndex=No
ConnSettings=
```

9. Save and close this file `odbc.ini`.
10. Enter **`odbcinst -I -s -f /usr/local/etc/odbc.ini`**.
    RESULT: The Data Source Name (DSN) of the driver is set up.
11. Open the file `/etc/canopy/canopyapi.xml`.
12. Find the string `<host xsi:type="xsd:string">localhost</host>`.
13. Replace `localhost` with **`psql`**.
14. Find the string `<type xsi:type="xsd:string">mysql</type>`.
15. Replace `mysql` with **`odbc`**.
    RESULT: The BAM server is configured for the engined process of BAM.
16. Find the following block of lines:

```
<radius xsi:type="canopy:Radius">
   <enabled xsi:type="xsd:boolean">trueorfalse</enabled>
   <primaryServer xsi:type="xsd:string">localhost</primaryServer>
   <secondaryServer
     xsi:type="xsd:string">localhost</secondaryServer>
   <portAlias xsi:type="xsd:string">radius</portAlias>
   <sharedSecret
     xsi:type="xsd:string">unsafe_password</sharedSecret>
   <maxRetries xsi:type="xsd:int">3</maxRetries>
   <timeOut xsi:type="xsd:int">3</timeOut>
   <networkInterface xsi:type="xsd:string">eth0</networkInterface>
   <canopyUserPassword
     xsi:type="xsd:string">please_change_me</canopyUserPassword>
 </radius>
```

17. In the second line of this block, ensure that *`trueorfalse`* is changed to **`false`**.
    RESULT: BAM disables RADIUS authentication.
18. Save the file `/etc/canopy/canopyapi.xml`.
19. Open the file `/usr/local/canopy/include/canopy.xml`.
20. Find the following block of lines:

```
<databases>
  <database host="localhost" name="GUInamestring" type="GUItypestring" />
</databases>
```

21. Change *`GUInamestring`* to **`canopy`**.
22. Change *`GUItypestring`* to **`pgsql`**.
    RESULT: The BAM GUI is set for a PostgreSQL database.
23. Save the file `/usr/local/canopy/include/canopy.xml`.
24. Enter **`/etc/rc.d/init.d/engined restart`**.
25. View the file `/var/log/canopy/canopy.log` to distinguish whether engined successfully connected to the database.
26. Log off as `root`.

Test the ODBC Driver for PostgreSQL

1. Enter **`isql psql canopy canopy`**.
2. Enter **`SELECT * from BAD_ESN`**.
   RESULT: Output resembles the following example (when no ESN data exists).

```
+-------------+----------------+--------------------------+-------------+
| esn         | num_bad_request| timestamp                | apa         |
+-------------+----------------+--------------------------+-------------+
+-------------+----------------+--------------------------+-------------+
```

USE A PostgreSQL DATABASE

PostgreSQL Directories

PostgreSQL uses the following directories on the BAM server:

- `/var/lib/pgsql`
- `/var/log/pgsql`
- `/usr/lib/pgsql`
- `/usr/share/pgsql`
- `/etc/sysconfig/pgsql`

PostgreSQL Documentation

PostgreSQL documentation is available at the following on-line resources:

- http://techdocs.postgresql.org/#convertfrom
- http://www.designharbor.com/Coding/opentut.php3?mn=&pn=t&id=67&page=1&
- http://wiki.ael.be/index.php/PostgresQL101

In addition, the following book is a helpful resource:

> *The Practical SQL Handbook: Using Structured Query Language (Third Edition)*
> by Judith S. Bowman, Sandra L. Emerson, Marcy Darnovsky
> Addison-Wesley Publishing Company
> ISBN 0-201-44787-8

Enable PostgreSQL on Red Hat Enterprise Linux Version 3

To enable PostgreSQL on the Red Hat Enterprise Linux Version 3 operating system, perform the following steps:

1. Select **System Settings→Server Settings→Services**.
2. Select **postgresql**.

3. Click the **Start** icon.
   RESULT: The system responds as follows:

```
Status: postmaster (pid n n ..) is running...
```

Configure PostgreSQL to Require Passwords

To impose password access on the PostgreSQL database, perform the following steps:

1. Log in as `root` or, at the shell prompt, enter **`su -`**.

With an editor utility, open the file `/var/lib/pgsql/data/pg_hba.conf`.

Find the following block of lines:

```
# TYPE   DATABASE    USER        IP-ADDRESS        IP-MASK           METHOD

local    all         all                                             md5
host     all         all         127.0.0.1         255.255.255.255   md5
```

Ensure that `md5` is the method for access to `local` and `host`, as desired.

Change Password for PostgreSQL

The default password on the Red Hat Enterprise Linux Version 3 operating system is set to `!!` in the file `/etc/shadow`. From a normal user account, to log in (or **`su`** to the PostgreSQL user), you must first perform the following steps that change the password as follows:

1. Log in as `root` or, at the shell prompt, enter **`su -`**.
2. Enter **`passwd postgres`**.
   The system responds as follows:

```
Changing password for user postgres.
New password:
```

3. Enter ***`postgres1`***, where *`postgres1`* is your chosen new password.
   The system repeats:

```
New password:
```

4. Re-enter ***`postgres1`***, where *`postgres1`* is your chosen new password, to confirm the new password setting.

Configure PostgreSQL to Use TCP/IP Sockets

To set PostgreSQL to use TCP/IP sockets, perform the following steps:

1. Log in as `root` or, at the shell prompt, enter **`su -`**.

With an editor utility, open the file `/var/lib/pgsql/data/postgresql.conf`.

Find the following block of lines:

```
#
#       Connection Parameters
#
tcpip_socket = trueorfalse
#ssl = false
```

2. Ensure that *`trueorfalse`* is changed to **`true`**.

Create Canopy User and Database

Perform the following steps to create a user named auth whose password is canopy, create a database named auth, and open a PostgreSQL session.

NOTE: This is the *only* method for administration of users for a PostgreSQL database.

1. Enter **`su - postgres`**.
2. Enter **`createuser auth -P canopy`**.
3. Enter **`createdb auth`**.
4. Enter **`psql -U auth -f /etc/canopy/canopypg.sql`**.

Use PostgreSQL Interactive Terminal Commands

The following interactive terminal commands are supported:

```
auth$ psql

auth-> \z
```

This command displays the access privileges for the database `auth` as follows:

```
 Schema |  Table  | Access privileges
--------+---------+-------------------
 public | ap      |
 public | bad_esn |
 public | ss      |

auth-> \h
```

This command displays the available help as follows:

```
  ABORT                      CREATE TABLE               EXECUTE
  ALTER DATABASE             CREATE TABLE AS            EXPLAIN
  ALTER GROUP                CREATE TRIGGER             FETCH
  ALTER TABLE                CREATE TYPE                GRANT
  ALTER TRIGGER              CREATE USER                INSERT
  ALTER USER                 CREATE VIEW                LISTEN
  ANALYZE                    DEALLOCATE                 LOAD
  BEGIN                      DECLARE                    LOCK
  CHECKPOINT                 DELETE                     MOVE
  CLOSE                      DROP AGGREGATE             NOTIFY
  CLUSTER                    DROP CAST                  PREPARE
  COMMENT                    DROP CONVERSION            REINDEX
  COMMIT                     DROP DATABASE              RESET
  COPY                       DROP DOMAIN                REVOKE
  CREATE AGGREGATE           DROP FUNCTION              ROLLBACK
  CREATE CAST                DROP GROUP                 SELECT
  CREATE CONSTRAINT TRIGGER  DROP INDEX                 SELECT INTO
  CREATE CONVERSION          DROP LANGUAGE              SET
  CREATE DATABASE            DROP OPERATOR CLASS        SET CONSTRAINTS
  CREATE DOMAIN              DROP OPERATOR              SET SESSION
```

```
AUTHORIZATION
  CREATE FUNCTION           DROP RULE                 SET TRANSACTION
  CREATE GROUP              DROP SCHEMA               SHOW
  CREATE INDEX              DROP SEQUENCE             START TRANSACTION
  CREATE LANGUAGE           DROP TABLE                TRUNCATE
  CREATE OPERATOR CLASS     DROP TRIGGER              UNLISTEN
  CREATE OPERATOR           DROP TYPE                 UPDATE
  CREATE RULE               DROP USER                 VACUUM
  CREATE SCHEMA             DROP VIEW
  CREATE SEQUENCE           END
```

`auth-> \?`

This command displays scrolling definitions of the *\command* set, as listed in the following table:

Command Syntax	Executed Result
\a	toggle between unaligned and aligned output mode
\c[onnect] ***DBNAME- USER***	connect to new database (currently `auth`)
\C ***STRING***	set table title, or unset if none
\cd ***DIR***	change the current working directory
\copy ...	perform SQL COPY with data stream to the client host
\copyright	show PostgreSQL usage and distribution terms
\d ***NAME***	describe table, index, sequence, or view
\d{t|i|s|v|S} ***PATTERN***	list {`tables/indexes/sequences/views/System`} tables
\d{t|i|s|v|S} ***PATTERN*** **+**	list {`tables/indexes/sequences/views/System`} `tables` (more detail)
\da ***PATTERN***	list aggregate functions
\dd ***PATTERN***	show comment for object
\dD ***PATTERN***	list domains
\df ***PATTERN***	list functions
\df ***PATTERN*** **+**	list functions (more detail)
\do ***NAME***	list operators
\dl	list large objects, same as **\lo_list**
\dp ***PATTERN***	list table access privileges
\dT ***PATTERN***	list data types
\dT ***PATTERN*** **+**	list data types (more detail)
\du ***PATTERN***	list users
\e ***FILE***	edit the query buffer (or *FILE*) with external editor

Command Syntax	Executed Result
\echo *STRING*	write *STRING* to standard output
\encoding *ENCODING*	show or set client encoding
\f *STRING*	show or set field separator for unaligned query output
\g *FILE*	send query buffer to server (and results to *FILE* or |pipe)
\h *NAME*	help on syntax of SQL commands, * for all commands
\H	toggle HTML output mode (currently off)
\i *FILE*	execute commands from *FILE*
\l	list all databases
\lo_export	export large object
\lo_import	import large object
\lo_list	list large object
\lo_unlink	unlink large object
\o *filename*	send all query results to file or |pipe
\p	show the contents of the query buffer
\pset *NAME VALUE*	set table output option, where *NAME* = `format|border|expanded|fieldsep|null| recordsep|tuples_only|title|tableattr| pager`
\q	quit `psql`
\qecho *STRING*	write *STRING* to query output stream (see **\o**)
\r	reset (clear) the query buffer
\s *FILE*	display history or save it to *FILE*
\set *NAME VALUE*	set internal variable, or list all if no parameters
\t	show only rows (currently off)
\T *STRING*	set HTML **<table>** tag attributes, or unset if none
\timing	toggle timing of commands (currently off)
\unset *NAME*	unset (delete) internal variable
\w *FILE*	write query buffer to *FILE*
\x	toggle expanded output (currently off)
\z *PATTERN*	list table access privileges (same as **\dp**)
\!	start interactive shell
\! *COMMAND*	execute *COMMAND* in shell

NOTE: A script is distributed with BAM Release 2.0 and later releases to create the ESN data table. When the script has been executed, the system responds as follows:

```
psql:dbtables-pg:11: NOTICE:  CREATE TABLE / PRIMARY KEY will create
implicit
index 'ss_pkey' for table 'ss'
CREATE TABLE
psql:dbtables-pg:18: NOTICE:  CREATE TABLE / PRIMARY KEY will create
implicit
index 'bad_esn_pkey' for table 'bad_esn'
CREATE TABLE
psql:dbtables-pg:24: NOTICE:  CREATE TABLE / PRIMARY KEY will create
implicit
index 'ap_pkey' for table 'ap'
CREATE TABLE

auth=> \l
```

This command displays a list of databases as follows:

```
   Name    |  Owner   | Encoding
-----------+----------+-----------
 auth      | postgres | SQL_ASCII
 template0 | postgres | SQL_ASCII
 template1 | postgres | SQL_ASCII

auth=> \d
```

This command displays a list of relations as follows:

```
 Schema |  Name   | Type  | Owner
--------+---------+-------+-------
 public | ap      | table | auth
 public | bad_esn | table | auth
 public | ss      | table | auth

auth=> \d ap
```

This command displays the table `public.ap` as follows:

```
 Column |          Type          |      Modifiers
--------+------------------------+---------------------
 apa    | character(12)          | not null default ''
 name   | character varying(255) |
 ip     | character varying(32)  |
Indexes: ap_pkey primary key btree (apa)
```

```
auth=> \d bad_esn
```

This command displays the table `public.bad_esn` as follows:

```
     Column      |            Type             |              Modifiers
-----------------+-----------------------------+---------------------------------------
 esn             | character(12)               | not null default ''
 num_bad_request | integer                     | not null default '0'
 timestamp       | timestamp without time zone | not null default '2001-01-01 12:00:00'
 apa             | character(12)               | not null default ''
Indexes: bad_esn_pkey primary key btree (esn)
```

Display Data

The recommended command to view data in the PostgreSQL database is as follows:

```
auth=> SELECT * from SS
```

If data already exists, this command displays the table `public.ss` as follows:

```
 Column |          Type          |      Modifiers
--------+------------------------+----------------------
 esn    | character(12)          | not null default ''
 skey   | character(32)          | not null default ''
 qos    | character(64)          | not null default ''
 tlt    | time without time zone | default '00:00:00'
 dlt    | date                   | default '2002-01-01'
 apa    | character(12)          | not null default ''
 res    | character(1)           | default ''
 tnar   | integer                | default '0'
 tnaf   | integer                | default '0'
Indexes: ss_pkey primary key btree (esn)
```

Reload PostgreSQL Configuration Data

To reload configuration data into the PostgreSQL database, enter the following command:

```
pg_ctl -D /var/lib/pgsql/data/ reload
```

Hazardous Command

The **DROP** commands are generally hazardous and should be avoided.

APPENDIX 2: MySQL DATABASE SUPPORT

SET UP BAM GUI FOR MySQL DATABASE

The version of MyODBC in the Red Hat Enterprise Linux Version 3 distribution cannot be used. To support a MySQL database, perform the following steps.

Distinctive fonts indicate

`literal user input.`
`variable user input.`
`literal system responses.`

1. Visit http://dev.mysql.com/downloads/connector/odbc/3.51.html.
2. Select and download **MyODBC-3.51.07-1.i586.rpm**.
3. As root, enter **`rpm -ivh MyODBC-3.51.07-1.i586.rpm`**.
4. If BAM and the MySQL database server will reside on the same computer, enter **`ln -s /var/lib/mysql/mysql.sock /tmp/mysql.sock`**. (For Red Hat, the domain socket is in a different path then what MySQL expects.)

The following procedure presumes that **unixODBC-2.2.8-2.3.0.2**, the database client, and the ODBC driver (**MyODBC-3.51.07-1.i586.rpm**) have been installed as documented above. If any package was incorrectly omitted or selected, you can use the add or remove function from the system menu to select or omit the package.

To set up a system-wide ODBC driver to use a MySQL database, perform the following steps on the client computer:

1. On the computer where engined/ssed will run, enter **`su -`** to log in as `root`.
2. Change directory to `/usr/local/etc/`.
3. Open or create the file `odbcinst.ini`.
4. Add the following lines to the file:

```
[MySQL]
Description=ODBC for MySQL
Driver=/usr/lib/libmyodbc3_r.so
FileUsage=1
```

5. Save and close the file `odbcinst.ini`.
6. Enter **`odbcinst -I -d -f /usr/local/etc/odbcinst.ini`**.
   RESULT: The ODBC driver is installed.
7. In the same directory (`/usr/local/etc/`), open or create the file `odbc.ini`.

8. Add the following lines to the file:

```
[mysql]
Description=MySQL for canopy
Driver=MySQL
Trace=Yes
TraceFile=/tmp/sql.log
User=canopy
Host=localhost (This can be a remote server)
Port=
Socket=
Database=04004SSE
```

9. Save and close this file `odbc.ini`.
10. Enter **`odbcinst -I -s -f /usr/local/etc/odbc.ini`**.
    RESULT: The Data Source Name (DSN) of the driver is set up.
11. Open the file `/etc/canopy/canopyapi.xml`.
12. Find the string `<host xsi:type="xsd:string">localhost</host>`.
13. Replace `localhost` with **`mysql`**.
14. Find the string `<type xsi:type="xsd:string">mysql</type>`.
15. Replace `mysql` with **`odbc`**.
    RESULT: The BAM server is configured for the engined process of BAM.
16. Find the following block of lines:

```
<radius xsi:type="canopy:Radius">
   <enabled xsi:type="xsd:boolean">trueorfalse</enabled>
   <primaryServer xsi:type="xsd:string">localhost</primaryServer>
   <secondaryServer
     xsi:type="xsd:string">localhost</secondaryServer>
   <portAlias xsi:type="xsd:string">radius</portAlias>
   <sharedSecret
     xsi:type="xsd:string">unsafe_password</sharedSecret>
   <maxRetries xsi:type="xsd:int">3</maxRetries>
   <timeOut xsi:type="xsd:int">3</timeOut>
   <networkInterface xsi:type="xsd:string">eth0</networkInterface>
   <canopyUserPassword
     xsi:type="xsd:string">please_change_me</canopyUserPassword>
 </radius>
```

17. In the second line of this block, ensure that *`trueorfalse`* is changed to **`false`**.
    RESULT: BAM disables RADIUS authentication.
18. Save the file `/etc/canopy/canopyapi.xml`.
19. Open the file `/usr/local/canopy/include/canopy.xml`.
20. Find the following block of lines:

```
<databases>
  <database host="localhost" name="GUInamestring" type="GUItypestring" />
</databases>
```

21. Change *`GUInamestring`* to **`04004SSE`**.

22. Change *GUItypestring* to **mysql**.
    RESULT: The BAM GUI is set for a MySQL database.
23. Save the file /usr/local/canopy/include/canopy.xml.
24. Enter **/etc/rc.d/init.d/engined restart**.
25. View the file /var/log/canopy/canopy.log to distinguish whether engined successfully connected to the database.
26. Log off as root.

Test the ODBC Driver for MySQL

1. Enter **isql mysql canopy canopy**.
2. Enter **SELECT * from BAD_ESN**.
   RESULT: Output resembles the following example (when no ESN data exists).

```
+-------------+----------------+---------------------------+-------------+
| esn         | num_bad_request| timestamp                 | apa         |
+-------------+----------------+---------------------------+-------------+
+-------------+----------------+---------------------------+-------------+
```

REPLICATE MySQL DATABASE ON REDUNDANT SERVER

In a Canopy network that deploys a redundant BAM server, automatic replication of the MySQL database on the redundant server is highly recommended. This ensures that the proper data transfer limits are applied to each SM even when the primary BAM server is out of service.

Caveats about Database Replication

In a multiple BAM server deployment, the redundant server(s) should not store any ESN data other than what is also present on the primary server. Records that are stored on only the redundant server are lost when the replication processes are completed.

On a live system, the primary BAM server is unavailable for authentication during the brief interval when the MySQL database is copied and the my.cnf configuration file is edited. Similarly, the redundant server is unavailable for the brief interval when the pre-existing database is being overwritten.

Set Up Automatic Replication

NOTE: The procedure in this section is based on instructions that are provided in the *MySQL Reference Manual* at http://www.mysql.com/documentation/index.html. Before you enable replication

- study the sections that relate to replication setup and administration.
- diverge from the following procedure where appropriate for the specifics of your system.

In BAM release 2.0 and later releases, the following procedure sets up replication between two servers that run MySQL software. Each server in this relationship is equal in authority—neither has permanent status as the server to be manually updated or as the server to be automatically updated. A manual update in one server triggers an automatic update in the other.

However, for this replication *set up* procedure, you must identify the server (Server 1) whose database is to be copied to the other (Server 2). As you do, ensure that the database in Server 2 does not contain SM information that should also be in Server 1.

This procedure uses examples for IP addresses, user names, and passwords. Table 8 relates these examples to the server designations. As you perform the steps, substitute IP addresses, user names, and passwords that are appropriate for your system.

Distinctive fonts indicate

literal user input.
variable user input.
literal system responses.

SUGGESTION: Use this table as a job aid to store the expressions that you will substitute for the examples.

Table 8: Example expressions for this procedure

Server ID	IP Address	User Name	User Password
Server 1	***10.0.0.1***	***server_1_repl***	***server_1_passwd***
Server 2	***10.0.0.2***	***server_2_repl***	***server_2_passwd***

Replication Setup on Server 1

To begin MySQL database replication setup, perform the following steps on Server 1:

1. In a shell interface to Server 1, enter **`mysql -u root`**.
   RESULT: The MySQL client program starts.
2. At the MySQL prompt, enter (with no line break)
   `grant file on *.* to` ***`server_2_repl`***`@`***`10.0.0.2`*** **`identified by '`**`server_2_passwd`**`';`**.
   RESULT: Access to Server 2 is granted on Server 1.
3. Enter **`exit`**.
   RESULT: The MySQL client program is closed.
4. At the shell prompt, enter **`su -`**.
   RESULT: The user mode is changed to root.
5. With an editor utility, open the file `/etc/my.cnf`.

6. Under the section titled `[mysqld]`, append the following seven lines:

```
port=3306
log-bin
server-id=1
master-host=10.0.0.2
master-user=server_1_repl
master-password=server_1_passwd
master-port=3306
```

7. Save the file `/etc/my.cnf`.
8. At the shell prompt, enter **`mysqladmin shutdown`**.
   RESULT: The MySQL administrator program is closed.
9. At the shell prompt, enter **`cd /var/lib/mysql`**.
10. Enter **`tar -cvf 04004SSE-snapshot-server_1.tar 04004SSE/`**.
    RESULT: The Canopy database is stored as a tar file.

    NOTE: The following steps presume that you use the **`sftp`** utility to transport the database to Server 2. Alternatively, you may transport the database by disk and write it under the `/var/lib/mysql` directory on Server 2.
11. Enter the following commands:

```
sftp root@10.0.0.2
cd /var/lib/mysql
put 04004SSE-snapshot-server_1.tar
exit
```

    RESULT: The database of Server 1 replaces the previous database on Server 2.
12. Enter **`safe_mysqld &`**.
    RESULT: The MySQL program is restarted.

Replication Setup on Server 2

To continue MySQL database replication setup, perform the following steps on Server 2:

1. In a shell interface to Server 1, enter **`mysql -u root`**.
   RESULT: The MySQL client program starts.
2. At the MySQL prompt, enter (with no line break)
   `grant file on *.* to server_1_repl@10.0.0.1 identified by 'server_1_passwd';`.
   RESULT: Access to Server 1 is granted on Server 2.
3. Enter **`exit`**.
   RESULT: The MySQL client program is closed.
4. At the shell prompt, enter **`su -`**.
   RESULT: The user mode is changed to root.
5. With an editor utility, open the file `/etc/my.cnf`.

6. Under the section titled `[mysqld]`, append the following seven lines:

```
port=3306
log-bin
server-id=2
master-host=10.0.0.1
master-user=server_2_repl
master-password=server_2_passwd
master-port=3306
```

7. Save the file `/etc/my.cnf`.
8. At the shell prompt, enter **`mysqladmin shutdown`**.
   RESULT: The MySQL administrator program is closed.
9. Optionally, to tar the Server 2 Canopy database for restoration
   a. enter **`cd /var/lib/mysql`**
   b. enter **`tar -cvf 04004SSE-snapshot-server_2.tar 04004SSE/`**.

   RESULT: The Canopy database is stored as a tar file.
10. Enter **`rm -rf 04004SSE`**.
    RESULT: The Server 2 Canopy database is deleted.
11. Enter **`tar -xvf 04004SSE-snapshot-server_1.tar`**.

    RESULT: The Server 1 Canopy database has replaced the Server 2 Canopy database on Server 2.
12. Enter **`safe_mysqld &`**.

    RESULT: The MySQL program is restarted. Replication is fully operational. Any change that is made in the database on one server is written to the database on the other server.

Replication Troubleshooting

The commands in this section are supported for troubleshooting the database replication process. First, perform the following steps:

1. In a shell interface to the server, enter **`mysql -u root`**.
   RESULT: The MySQL client program starts.
2. At the MySQL prompt, enter **`use mysql;`**.
   RESULT: The database is set to mysql.

Now any of the following commands can be executed:

- **`select Host, User, Password from user;`**

  RESULT: The response should provide the IP address and replication user name for the other server.

- **`show master status;`**

  RESULT: The master log file name and position should be identical to the slave log file name and position on the other server.

- **`show slave status \G`**

  RESULT: The slave log file name and position should be identical to the master log file name and position on the other server.

- **`show processlist \G`**

RESULT: A process should list the User and Host entries that match the replication user name and host IP address of the other server.

Replication Removal on Server 1

The following procedures are provided for the case where you want to disable the replication feature. To begin the removal of MySQL database replication, perform the following steps on Server 1:

1. At the shell prompt, enter **`mysqladmin shutdown`**.
   RESULT: The MySQL administrator program is closed.
2. With an editor utility, open the file `/etc/my.cnf`.
3. Under the section titled `[mysqld]`, delete the following seven lines:

```
port=3306
log-bin
server-id=1
master-host=10.0.0.2
master-user=server_1_repl
master-password=server_1_passwd
master-port=3306
```

4. Save the file `/etc/my.cnf`.
5. Enter **`cd /var/lib/mysql`**.
6. Enter **`rm *-bin.*`**.
   RESULT: The replication bin files are removed.
7. Enter **`rm master.info`**.
   RESULT: The replication master info file is removed.
8. Enter **`rm 04004SSE-snapshot-server_1.tar`**.
   RESULT: The tarred copy of the Canopy database is removed.
9. Enter **`safe_mysqld &`**.
   RESULT: The MySQL program is restarted.
10. Enter **`mysql -u root`**.
    RESULT: The MySQL client program starts.
11. At the MySQL prompt, enter (with no line break)
    `revoke file on *.* from server_2_repl@10.0.0.2 identified by 'server_2_passwd';`.
    RESULT: The file privileges that Server 2 had on Server 1 are removed.
12. Enter (with no line break) **`delete from user where User = 'server_2_repl' and Host = '10.0.0.2';`**.
    RESULT: The replication user of Server 2 is deleted from Server 1.
13. Enter **`flush privileges;`**.
    RESULT: The removal of privileges is put into effect.
14. Enter **`exit`**
    RESULT: The MySQL client program is closed.

Replication Removal on Server 2

To continue the removal of MySQL database replication, perform the following steps on Server 2:

1. At the shell prompt, enter **`mysqladmin shutdown`**.
   RESULT: The MySQL administrator program is closed.
2. With an editor utility, open the file `/etc/my.cnf`.
3. Under the section titled `[mysqld]`, delete the following seven lines:

```
port=3306
log-bin
server-id=1
master-host=10.0.0.1
master-user=server_2_repl
master-password=server_2_passwd
master-port=3306
```

4. Save the file `/etc/my.cnf`.
5. Enter **`cd /var/lib/mysql`**.
6. Enter **`rm -rf 04004SSE`**.
   RESULT: The Canopy database is deleted.
7. Enter **`tar -xvf 04004SSE-snapshot-server_2.tar`**.
   RESULT: The original tarred copy from Server 2 replaces deleted Canopy database.
8. Enter **`rm 04004SSE-snapshot-server_1.tar`**.
   RESULT: The snapshot of the Server 1 database is removed.
9. Enter **`safe_mysqld &`**.
   RESULT: The MySQL program is restarted.
10. Enter **`mysql -u root`**.
    RESULT: The MySQL client program starts.
11. At the MySQL prompt, enter (with no line break)
    `revoke file on *.* from server_1_repl@10.0.0.1 identified by 'server_1_passwd';`.
    RESULT: The file privileges that Server 1 had on Server 2 are removed.
12. Enter (with no line break) **`delete from user where User = 'server_1_repl' and Host = '10.0.0.1';`**.
    RESULT: The replication user of Server 1 is deleted from Server 2.
13. Enter **`flush privileges;`**.
    RESULT: The removal of privileges is put into effect.
14. Enter **`exit`**.
    RESULT: The MySQL client program is closed.

VERIFY BAM REDUNDANCY

Test the redundancy of BAM data as follows:

1. On Server 1, insert or change data for a test SM.
2. On Server 2, verify that the data is as entered in Server 1.

APPENDIX 3: SSE COMMAND-LINE INTERFACE

The following sections list and describe SSE commands to interface with the MySQL or PostgreSQL database. For further information about

- PostgreSQL databases, see the index of PostgreSQL documentation at http://www.postgresql.org/docs.
- MySQL databases, see *MySQL® Reference Manual* at http://www.mysql.com/documentation/index.html.

CAVEATS

To avoid commonly experienced errors, observe the following caveats about command-line entries:

- `telnet` commands are used to configure SM data and configure or administer users and passwords for `telnet` access to the SSE interface.
- ESNs are entered *without dashes* in these commands.
- The Canopy system maintains `telnet` ports in `/etc/services`.
- The SSE port, Port 9080, is aliased as `sse`.

SSE DATABASE COMMANDS

This section provides the database commands for use with the SSE interface, and defines the allowed usage for each command. At any time, you can enter **`help`** at the `sse` prompt to view these lists.

Distinctive fonts indicate

`literal user input.`
`variable user input.`
`literal system responses.`

`cmd show version`
Display the version of SSE software that is installed.

`cmd show esn`
Display all ESNs with related information.

`cmd show esn` ***`esn`***
Display the specified ESN (in hexadecimal format without dashes) with related information. ***esn*** must be expressed in hexadecimal format.

EXAMPLE:
`cmd show esn 1f2a3f4e3d22`

`cmd show config`
Display all configuration values that the database uses. This command calls the `show variables` SQL command.
NOTE: This command is deprecated in BAM Release 2.0 and later releases.

`cmd show all`
Display all configuration values and statistics that are in the database. This command calls the `cmd show config` SSE command.
NOTE: This command is deprecated in BAM Release 2.0 and later releases.

`cmd clear esn counter` ***`esn`***
Reset the counter to zero for the specified ESN (in hexadecimal format without dashes).

EXAMPLE:
`cmd clear esn counter 1f2a3f4e3d22`

`config save table` ***`/path/filename.txt`***
Save the ESN data from the database to the specified path and file.
NOTE: This syntax (**`table`**) is for execution in only Releases 1.0 and 1.1.

`config save database` ***`/path/filename.txt`***
Save the ESN data from the database to the specified path and file.
NOTE: This syntax (**`database`**) is for execution in only Releases 2.0 and later. The format of SSE database in Releases 1.0 and 1.1 is incompatible with Release 2.0. However, the BAM GUI can be used to import the Release 1.0 or 1.1 format for use with Release 2.0.

`config upload table` ***`/path/filename.txt`***
Upload a properly formatted ESN data file from the specified path to the database.
NOTE: This syntax (**`table`**) is for execution in only Releases 1.0 and 1.1.

`config upload database` ***`/path/filename.txt`***
Upload a properly formatted ESN data file from the specified path to the database.
NOTE: This syntax (**`database`**) is for execution in only Releases 2.0 and later.

`config add esn` ***`esn skey suldr sdldr ulba dlba`***
Add the specified ESN with the specified arguments into the database.

FORMATS:

`esn`	hexadecimal without dashes. For example, **`1f2a3f4e3d22`**.
`skey`	either **`0`** for the default key or a unique 32-character hexadecimal number for a non-default key.
`suldr`	**Sustained Uplink Data Rate** in the range **`0`** to **`10000`** kbps.
`sdldr`	**Sustained Downlink Data Rate** in the range **`0`** to **`10000`** kbps.
`ulba`	**Uplink Bandwidth Allocation** in the range **`0`** to **`500000`** kbits.
`dlba`	**Downllink Bandwidth Allocation** in the range **`0`** to **`500000`** kbits.

`config modify esn` ***`esn skey suldr sdldr ulba dlba`***
Update the specified ESN with the specified arguments in the database.
NOTE: This command is for execution in only Releases 2.0 and later. Formats are as defined above.

`config disable esn` ***`esn`***
Disable the specified ESN in the database.
NOTE: This command is for execution in only Releases 2.0 and later.

`config enable esn` ***`esn`***
Enable the specified ESN in the database.
NOTE: This command is for execution in only Releases 2.0 and later.

`config delete esn` ***`esn`***
Remove the specified ESN from the database.

The following command erases all data in the remote database before the copy execution.

`config copy to database` ***`ip user password`***
Copies configuration data from port on the network element that is identified by ***`ip`*** into the database. To do so, identify the ***`user`*** and ***`password`*** that the database has stored.
NOTE: This command is deprecated in BAM Release 2.0 and later releases.

SSE TELNET COMMANDS

This section provides the `telnet` commands for use with the SSE interface, and defines the allowed usage for each command. At any time, the operator can enter **`help`** at the `sse` prompt to view these lists.

Distinctive fonts indicate

`literal user input.`
`variable user input.`

`telnet` ***`localhost`*** **`sse`**
Initiate a `telnet` session in the SSE interface. The default user name is **`root`**. The default password is **`root`**.

`config add user` ***`user password password`***
Insert a new SSE `telnet` user into the user list. The second instance of ***`password`*** is a required confirmation. By default, a new user is given both read and write access. To restrict access to read-only, use the **`config modify level`** ***`user level`*** command as documented below.

`config delete user` ***`user`***
Remove the specified ***`user`*** from the user list. The user name is required as an argument.

`config store user`
Save changes to the SSE `telnet` user list.
NOTE: (This command is deprecated in BAM Release 2.0 and later releases.)

`config change pass` ***`user password password`***
Change the password for the specified ***`user`*** in the SSE `telnet` user list. The first instance of ***`password`*** is the new password. The second instance of ***`password`*** is a required confirmation of the new password.

`config modify level` ***`user level`***
Change the level of the ***`user`*** from either the default Level 2 or a level previously set by this command. Level 1 allows only read access. Level 2 allows both read and write access. Level 3 allows administrator privileges.

EXAMPLE:
`config modify level patquinn 1`

`help`
Display the full list of supported SSE commands.

`exit`
Conclude and leave the SSE `telnet` session, but allow the server to continue to operate on software.

APPENDIX 4: RADIUS SERVER SUPPORT

BAM Release 2.0 and later releases support the maintenance of SM authentication and bandwidth configuration on a Remote Authentication Dial-in User Service (RADIUS) server. In this case, the BAM server acts as the proxy or terminal server between the AP and the RADIUS server. These releases have been certified to support either

- FreeRADIUS (see http://www.freeradius.org/)
- Steel-Belted Radius® (see http://www.funk.com)[12]

The BAM server receives from RADIUS (and passes to the AP) the authentication and bandwidth configuration of the SM. Although neither the BAM GUI nor the AP can view or change the configuration on the RADIUS server, the BAM server is essential (cannot be bypassed) for the proxy role.

BAM and concurrent Canopy system software releases currently

- *do not* introduce any new MIB objects for monitoring or managing data on the RADIUS server.
- *do not* support the *RADIUS Authentication Client MIB*, RFC 2618.
- *do not* support the *RADIUS Authentication Server MIB*, RFC 2619.

RADIUS FIELDS IN canopyapi.xml

Definitions of the RADIUS fields in the file `/etc/canopy/canopyapi.xml` are provided in Table 9.

Table 9: RADIUS fields

Tags	Meaning of Values
<radius></radius>	RADIUS-specific properties
<enabled></enabled>	Whether RADIUS is enabled. **true** means radius is enabled.
<primaryServer></primaryServer>	IP Address of the primary RADIUS server.
<secondaryServer></secondaryServer>	IP Address of the secondary RADIUS server.
<portAlias></portAlias>	Alias for the RADIUS server.
<sharedSecret></sharedSecret>	Shared secret between the BAM and the RADIUS Server. This secret is also specified on the RADIUS server.
<maxRetries></maxRetries>	Number of retries for the BAM to send a message to the RADIUS server.
<timeOut></timeOut>	Time to elapse between retries.

[12] Steel-Belted Radius is a registered trademark of Funk Software, Inc.

Tags	Meaning of Values
<networkInterface></networkInterface>	Network interface type. Typically, the value is **eth0** for Ethernet.
<canopyUserPassword></canopyUserPassword>	Password that every subscriber enters for authentication by the RADIUS server. For each SM in the RADIUS database, this identical password must be specified. In FreeRADIUS, this corresponds to the field User-Password for each Subscriber.

SET UP RADIUS ON BAM SERVER

To set up the BAM server to defer bandwidth and authentication to a RADIUS server, perform the following steps.

Distinctive fonts indicate

`literal user input.`
`literal system responses.`
`variable system responses.`

1. Log in as `root` or, at the shell prompt, enter **`su -`**.
2. With an editor utility, open the file `/etc/canopy/canopyapi.xml`.
3. Find the following block of lines:

```
<radius xsi:type="canopy:Radius">
   <enabled xsi:type="xsd:boolean">trueorfalse</enabled>
   <primaryServer xsi:type="xsd:string">localhost</primaryServer>
   <secondaryServer
     xsi:type="xsd:string">localhost</secondaryServer>
   <portAlias xsi:type="xsd:string">radius</portAlias>
   <sharedSecret
     xsi:type="xsd:string">unsafe_password</sharedSecret>
   <maxRetries xsi:type="xsd:int">3</maxRetries>
   <timeOut xsi:type="xsd:int">3</timeOut>
   <networkInterface xsi:type="xsd:string">eth0</networkInterface>
   <canopyUserPassword
     xsi:type="xsd:string">please_change_me</canopyUserPassword>
 </radius>
```

4. In the second line of this block, set *`trueorfalse`* to **`true`**.
   RESULT: BAM enables RADIUS authentication.
5. In the `primaryServer` field, insert the IP address of the primary RADIUS server.
6. In the `secondaryServer` field, insert the IP address of the secondary RADIUS server.
7. In the `portAlias` filed, enter the alias for the RADIUS server.
8. In the `sharedSecret` field, enter the secret to share with the RADIUS server.

9. In the `maxRetries` field, enter how many times BAM should retry to send a message to the RADIUS server when attempts are failing.
10. In the `timeOut` field, enter how much time should elapse between retries.
11. In the `networkInterface` field, enter the type of network interface. (See Table 9.)
12. In the `canopyUserPassword` field, enter the one password that every SM in the RADIUS database should send for authentication.
13. Save the file `/etc/canopy/canopyapi.xml`.

SET UP BAM ON RADIUS SERVER

To set up RADIUS to interact with BAM software and store SM configuration data, perform the following steps.

NOTE: The Canopy BAM distribution includes the `directory.mot.com` file.

Distinctive fonts indicate

literal user input.
variable user input.
literal system responses.

1. With an editor utility, open the file `/etc/raddb/client.conf`.
2. For each BAM server, insert the following block of lines:

```
client BAMServerIPAddress {
    secret      = FromStep8Above
    shortname   = DesiredAliasForBAMServer
}
```

3. Save the file `/etc/raddb/client.conf`.
4. Open the file `/etc/raddb/users`.
5. For each SM for which the BAM server will forward authentication requests, insert the following block of lines:

```
SM_MACAddress Auth-Type := Local, User-Password == "FromStep12Above"
                  Motorola-Canopy-Shared-Secret = "AuthenticationKey",
                  Motorola-Canopy-SULDR = "SustainedUplinkDataRate",
                  Motorola-Canopy-SDLDR = "SustainedDownlinkDataRate",
                  Motorola-Canopy-ULBA = "UplinkBurstAllocation",
                  Motorola-Canopy-DLBA = "DownlinkBurstAllocation",
                  Fall-Through = Yes
```

For example:

```
0a003e000b4d Auth-Type := Local, User-Password == "please_change_me"
                        Motorola-Canopy-Shared-Secret = "deadbeef",
                        Motorola-Canopy-SULDR = "2200",
                        Motorola-Canopy-SDLDR = "7800",
                        Motorola-Canopy-ULBA = "4400",
                        Motorola-Canopy-DLBA = "15600",
                        Fall-Through = Yes
```

6. Save the file `/etc/raddb/users`.
7. Open the file `/etc/raddb/dictionary`.
8. Insert the following line:

   `$INCLUDE /etc/raddb/dictionary.mot.com`

9. Save the file `/etc/raddb/dictionary`.
10. In directory `/etc/raddb`, copy the file `directory.mot.com` from the Canopy BAM distribution.
    NOTE: This file specifies the bandwidth parameter types that are assigned values in the `/etc/raddb/users` file above.

APPENDIX 5: TROUBLESHOOTING

Problems and possible causes are listed in Table 10.

Table 10: Example problems for troubleshooting

Problem	Possible Cause
Some recent settings were lost and/or errors were generated.	Using the browser Back button. In any BAM GUI session, to return to a previously loaded BAM web page, use the **back** button in the GUI rather than the Back button of your browser.
MySQL driver used with BAM Release 1.1 does not work with BAM Release 2.0.	MySQL drivers cannot work with BAM Release 2.0. Access to the database is possible through only the ODBC interface.
BAM server will not start.	No BAM server floating license is available to assign in the licence management server. Check the BAM logs for the message `Unable to check out license for feature BAM.`[1]
APs cannot call the BAM server.	A port configuration or firewall restriction may be improperly set. See Table 4 on Page 10.
An SM in a newly deployed sector cannot register.	No AP authentication floating license is available to assign the newly deployed AP in the license manager server. Check the BAM logs for the message `Unable to check out license for feature AccessPoint.`[1]

1. This message is logged in file `businessrules/FlexLicenseManager.cpp`.

OTHER MESSAGES

The following other messages are logged in file `businessrules/FlexLicenseManager.cpp`:

- Message: `License checked out for feature BAM, version 2.0`
- Message: `License checked out for feature AccessPoint, version 2.0`

The following message is logged in file `businessrules/AccessPoint.cpp`:

- Message: `Access Point MACaddress on DottedIPAddress has checked out a license`